

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-283268

(43) 公開日 平成10年(1998)10月23日

(51) Int.Cl. <sup>6</sup>	識別記号	F I	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
G 0 6 K 17/00		G 0 6 K 17/00	E
19/10		G 0 9 C 1/00	6 3 0 E
G 0 9 C 1/00	6 3 0		6 3 0 B
		G 1 1 B 20/10	H
審査請求 未請求 請求項の数26 O L (全 20 頁) 最終頁に続く			

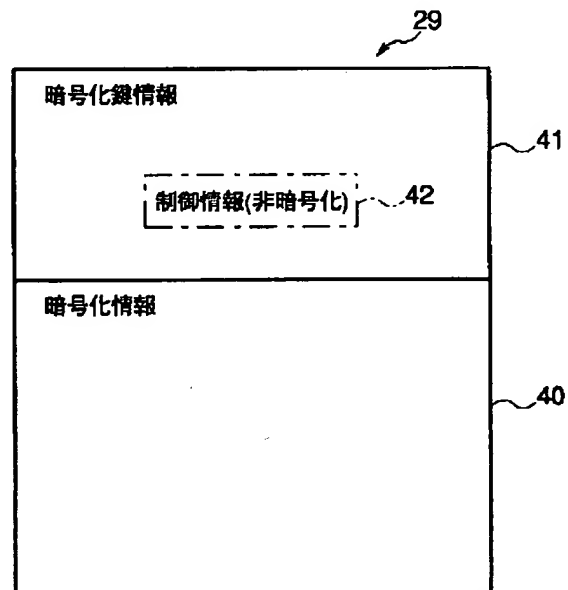
(21) 出願番号	特願平10-23284	(71) 出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22) 出願日	平成10年(1998)2月4日	(72) 発明者	山田 尚志 神奈川県川崎市幸区柳町70番地 株式会社 東芝柳町工場内
(31) 優先権主張番号	特願平9-25303	(72) 発明者	安東 秀夫 神奈川県川崎市幸区柳町70番地 株式会社 東芝柳町工場内
(32) 優先日	平9(1997)2月7日	(74) 代理人	弁理士 鈴江 武彦 (外6名)
(33) 優先権主張国	日本 (J P)		

(54) 【発明の名称】 情報記録媒体、記録装置、情報伝送システム、暗号解読装置

(57) 【要約】

【課題】 この発明は、情報記録媒体 (29、17a) からの暗号化情報 (40) の復号化を行う際に、セキュリティ確保が必要であるかまたは著作権確保が必要な情報に関する不正な複製の防止を行うことができる。

【解決手段】 この発明は、情報記録媒体 (29、17a) に、暗号化されている暗号化情報 (40) と、この暗号化情報 (40) を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報 (41) に、非暗号化された状態で上記暗号化情報 (40) を復号化する際の条件情報 (42) が記録されるようにし、その情報記録媒体 (29、17a) からの暗号化情報 (40) の復号化を暗号化鍵情報 (41) と条件情報 (42) とを用いて I C カード (4) 内にて行うようにしたものである。



## 【特許請求の範囲】

【請求項1】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報と、が記録される情報記録媒体において、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する場合の条件情報が記録されることを特徴とする情報記録媒体。

【請求項2】 上記条件情報が、上記暗号化情報の暗号化の許可を示す条件であることを特徴とする請求項1に記載の情報記録媒体。

【請求項3】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報を含むものであることを特徴とする請求項2に記載の情報記録媒体。

【請求項4】 上記条件情報が、領域情報を含むものであることを特徴とする請求項2に記載の情報記録媒体。

【請求項5】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項2に記載の情報記録媒体。

【請求項6】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項2に記載の情報記録媒体。

【請求項7】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報であることを特徴とする請求項1に記載の情報記録媒体。

【請求項8】 上記条件情報が、領域情報を含むものであることを特徴とする請求項7に記載の情報記録媒体。

【請求項9】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項7に記載の情報記録媒体。

【請求項10】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項7に記載の情報記録媒体。

【請求項11】 上記条件情報が、領域情報であることを特徴とする請求項1に記載の情報記録媒体。

【請求項12】 上記条件情報が、時間的情報を含むものであることを特徴とする請求項11に記載の情報記録媒体。

【請求項13】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項11に記載の情報記録媒体。

【請求項14】 上記条件情報が、時間的情報であることを特徴とする請求項1に記載の情報記録媒体。

【請求項15】 上記条件情報が、ユーザを限定する情報を含むものであることを特徴とする請求項14に記載の情報記録媒体。

【請求項16】 上記条件情報が、ユーザを限定する情報であることを特徴とする請求項1に記載の情報記録媒

体。

【請求項17】 暗号化鍵原案情報と復号化する場合の条件情報とを設定する設定手段と、

この設定手段により設定された暗号化鍵原案情報と非暗号化された状態の条件情報とにより暗号化鍵情報を生成する第1の生成手段と、

共通鍵情報を記録する記録手段と、

上記第1の生成手段により生成された暗号化鍵情報を上記記録手段に記録されている共通鍵情報により復号化して鍵情報を生成する第2の生成手段と、

暗号化する情報を入力する入力手段と、

この入力手段により入力された暗号化する情報を上記第2の生成手段により生成された鍵情報により暗号化して暗号化情報を生成する第3の生成手段と、

上記第1の生成手段により生成された条件情報を含む暗号化鍵情報と上記第3の生成手段により生成された暗号化情報とが対応した状態で情報記録媒体に記録する記録手段と、

を具備したことを特徴とする記録装置。

【請求項18】 上記条件情報が、上記暗号化情報の暗号化の許可を示す条件であることを特徴とする請求項17に記載の記録装置。

【請求項19】 上記条件情報が、上記暗号化情報の伝送経路や上記暗号化情報を暗号化された情報を用いる機器を示す機器情報条件であることを特徴とする請求項17に記載の記録装置。

【請求項20】 上記条件情報が、領域情報であることを特徴とする請求項17に記載の記録装置。

【請求項21】 上記条件情報が、時間的情報であることを特徴とする請求項17に記載の記録装置。

【請求項22】 上記条件情報が、ユーザを限定する情報であることを特徴とする請求項17に記載の記録装置。

【請求項23】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体を有する第1の装置と、この第1の装置と通信回線を介して接続され、上記第1の装置の情報記録媒体からの暗号化情報と暗号化鍵情報とが伝送される第2の装置とからなる情報伝送システムにおいて、

上記第1の装置の情報記録媒体に記録される暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録され、

上記第1の装置が、

上記情報記録媒体に記録されている条件情報を含む暗号化鍵情報と暗号化情報とを上記第2の装置へ送信する送信手段からなり、

上記第2の装置が、

上記第1の装置からの条件情報と暗号化鍵情報と暗号化情報とを復号化の処理を行う処理媒体に出力する第1の

出力手段と、  
 上記処理媒体からの復号化された情報に応じて処理を実行する実行手段からなり、  
 上記処理媒体が、  
 上記第 2 の装置からの条件情報に基づいて復号化を許可するか否かを判断する判断手段と、  
 この判断手段により復号化の許可を判断した際に、上記第 2 の装置からの暗号化鍵情報に基づいて暗号化情報を復号化する復号化手段と、  
 この復号化手段により復号化された情報を上記第 2 の装置へ出力する第 2 の出力手段とからなる、  
 ことを特徴とする情報伝送システム。

【請求項 2 4】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、  
 第 1 の特定情報と共通鍵情報とにより生成される第 2 の特定情報を記録している記録手段と、  
 第 1 の特定情報を設定する設定手段と、  
 この設定手段により設定される第 1 の特定情報と上記記録手段に記録されている第 2 の特定情報とにより上記共通鍵情報を生成する生成手段と、  
 上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第 1 の復号化手段と、  
 上記暗号化情報を上記第 1 の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第 2 の復号化手段と、  
 を具備したことを特徴とする暗号解読装置。

【請求項 2 5】 暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱う携帯可能媒体において、  
 第 1 の特定情報と共通鍵情報とが入力される入力部と、  
 この入力部から入力される第 1 の特定情報と共通鍵情報とにより第 2 の特定情報を生成する第 1 の生成手段と、  
 この第 1 の生成手段により生成される第 2 の特定情報を記録する記録手段と、  
 この記録手段への記録後、上記入力部からの入力を禁止する禁止手段と、  
 第 1 の特定情報を設定する設定手段と、  
 この設定手段により設定される第 1 の特定情報と上記記録手段に記録されている第 2 の特定情報とにより上記共通鍵情報を生成する第 2 の生成手段と、  
 上記暗号化鍵情報を上記第 2 の生成手段により生成される共通鍵情報により復号化して鍵情報を得る第 1 の復号化手段と、  
 上記暗号化情報を上記第 1 の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第 2 の復号化手段と、  
 を具備したことを特徴とする暗号解読装置。

【請求項 2 6】 暗号化されている暗号化情報と、この

暗号化情報を復号化する際の条件情報を含み上記暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、  
 第 1 の特定情報と共通鍵情報とにより生成される第 2 の特定情報を記録している記録手段と、  
 第 1 の特定情報を設定する設定手段と、  
 この設定手段により設定される第 1 の特定情報と上記記録手段に記録されている第 2 の特定情報とにより上記共通鍵情報を生成する生成手段と、  
 上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第 1 の復号化手段と、  
 上記暗号化情報を上記第 1 の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第 2 の復号化手段と、  
 上記条件情報により復号化を許可するか否かを判断する判断手段と、  
 この判断手段により判断結果に基づき、上記第 1、第 2 の復号化手段による復号化の実行を制御する制御手段と、  
 を具備したことを特徴とする暗号解読装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体、この情報記録媒体の記録装置、情報記録媒体からの情報を他の機器へ伝送して復号化する情報伝送システム、暗号化情報を暗号化鍵情報により元の情報に解読する暗号解読装置に関する。

【0002】

【従来の技術】 現在、インターネットを用いて世界中の情報入手が可能となっている。最近では特定ドメイン（領域、地域）内での情報サービスに対する課金システムも一部実施段階に入っている。そのインターネット普及とともに不正防止を目的としたセキュリティ確保も急務となっている。

【0003】 確保すべきセキュリティの対象として、  
 A) サービスを受けるユーザーを特定し、第 3 者が情報伝達経路の途中に入り込みサービス情報の横取りする事を防止する場合（情報横取りの防止）と、  
 B) 著作権を侵害してサービスプロバイダー以外の第 3 者が元のサービス情報を他の商業目的に利用するのを防止する場合（情報複製の防止）が有る。

【0004】 特に（B）に上げた情報複製防止に関する要請が今後急速に増加されることが予想される。これは、現在、ネットワークコンピュータの開発が精力的に進められているためである。

【0005】 現在開発中のネットワークコンピュータは、HDD を内蔵せず、OS さえも起動時に無線でホス

トサーバから呼び出し、作業に必要なアプリケーションソフトを必要な時、必要な機能プログラムを無線でインストールしながら作業を行う物である。

【0006】従って、従来はユーザが種々のアプリケーションパッケージソフトを購入し、HDDにインストールして使っている。しかし、ネットワークコンピュータを利用した場合には、事前の購入は不要となり、必要な時、必要な機能プログラムを呼び出して使うとともに、機能プログラムを呼び出す毎に課金されるシステムとなる。この機能プログラムは、パッケージプログラムのような大規模なプログラムでは無くJAV Aなどで記述された機能限定された非常に小規模なプログラムである。

【0007】したがって、ネットワークコンピュータを用いた場合には課金方法の特殊性から、ユーザによる機能プログラムの複製・再利用を禁止する必要がある。上記セキュリティ確保の方法として、アシンメトリック（対象暗号系）な暗号化技術を用いる、以下の3つの方法がある。

1. ユーザ側で公開鍵と秘密鍵を発行し、情報サービスプロバイダに対して情報サービス請求とともに公開鍵を通信する。
2. 情報サービスプロバイダがユーザから送ってもらった公開鍵に基付きサービス情報を暗号化してユーザに送る。
3. ユーザ側で自分の発行した秘密鍵を用いて暗号化情報を復号化して利用する。

【0008】しかし、これらの方法を用いた場合には、情報サービスプロバイダはユーザからの要求がある度に暗号化する必要が生じ、サービスコストが大幅にかかってしまう。

【0009】それを回避する方法として、暗号化と復号化時に共通な共通鍵を用いたシンメトリック（非対象暗号系）方式を採用し、暗号化されたサービス情報と同時に暗号化した共通鍵をユーザに送り、共通鍵を知っているユーザのみが解読できるシステムを採用する方法もある。

【0010】しかし、この方法を用いた場合には、以下の問題が生じる。

- a) ユーザにサービス情報をHDDや光ディスクに複製されてしまい、ネットワークコンピュータのように、情報サービス毎に課金出来ない。
- b) 共通鍵を一致させる限り、情報サービスプロバイダ以外の第3者が暗号化されたままの情報を不正に商業用に転用する事が容易となる。

【0011】以上の説明においてコンピュータネットワークを用いた情報サービスについて主に説明をしてきたが、同様に衛星放送を用いたサービスも存在する。放送を用いた場合にはアシンメトリック方式（公開鍵・秘密鍵を用いた方法）は使えず公開鍵を用いたシンメトリック方式を採用して、公開鍵を知っている特定ユーザーの

みがサービスを受けられるように出来る。

【0012】しかしこの場合にも上記の(a) (b)の問題が共通に発生する。また、以上の問題点を暗号化技術の観点から明示する。従来知られているように送付元と受信先が同じ鍵を使用する共通鍵（シンメトリック）方式では、以下の3つの欠点がある。

- 1) 鍵の転送中に第3者による不正コピーされる危険性がある。
- 2) 鍵の管理が複雑である。
- 3) 受信先で暗号データー自体の改ざんが容易に出来る。すなわち、受信先で暗号データーを共通鍵で復号化後、改竄した後、再度共通鍵で暗号化することが用意にできる。

【0013】これに対して、公開鍵と秘密鍵を用いたアシンメトリック方式では上記の問題点は改善されるが、以下のような欠点がある。

- イ] 暗号化／復号化の処理に膨大な時間がかかる。
- ロ] 情報サービスプロバイダがユーザに情報を送る毎にCAセンタ（認証局）にユーザ毎の公開鍵を問い合わせる必要がある。

【0014】という情報サービスプロバイダ側の負担が増大する。さらに、

- ハ] 秘密鍵の保管に関してユーザに多大な負担を掛ける。

【0015】たとえば、秘密鍵を盗まれただけで、セキュリティ確保は不可能となる。またユーザ側で、秘密鍵の入っているFDやICカードを容易に複製できるので、複製された秘密鍵情報が悪用される危険性がある。

【0016】と言う問題も有る。上記問題を改良する方法として、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するというハイブリッド方式が提案されている。この方式を用いれば、“[イ] 暗号化／復号化の処理時間の肥大化”は、緩和されるが、[ロ]と[ハ]の煩雑さは軽減されない。

【0017】また、情報を暗号化して伝送または記録するシステムにおいて、情報の暗号化に用いた鍵をも伝送または記録する場合には、鍵を秘匿するために暗号化に用いた鍵をそのまま伝送または記録することはせずに、鍵を情報の暗号化手段とは別の暗号化手段により別途暗号化した鍵情報として伝送または記録する。情報再生側では、まず鍵情報を鍵の復号化手段で復号化して得られた鍵を用いて、暗号化情報を情報の復号化手段により復号化する。

【0018】このことを利用し、暗号化前の鍵の中に再生制御情報を含ませるようにして、再生制御情報の改ざんを防ぐ方法が考えられる。しかしながら、この方法だと情報再生側において、再生制御情報を知るために鍵情報を復号化しなければならず、そのことが次のような情報再生システムの場合に大きな問題となる。

【0019】例えば、鍵情報の復号化手段も暗号化情報

の復号化手段も持たず、単に記録されたデータを読み取るだけのディスクドライブ装置に再生禁止情報を判定させ、復号化手段を持つ情報再生装置へのデータ転送を制御させるようにした情報再生システムについて説明する。

【0020】この場合、ディスクドライブ装置にも鍵情報の復号化手段を持たせなければならず、ディスクドライブ装置のコスト増加を招くことはもちろん、ディスクドライブ装置には不必要な鍵情報を復号化する復号化手段を持たせることによる、システム全体のセキュリティの低下を招くという深刻な問題を引き起こすからである。

【0021】

【発明が解決しようとする課題】この発明の目的は、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。この発明の目的は、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0022】この発明の目的は、共通鍵方式の欠点に対して、鍵の転送中の第三者による不正コピーされる危険性が少なく、鍵の管理が容易で、受信先での暗号データの改ざんが難しいと言う点が大幅に改善される。

【0023】この発明の目的は、アシンメトリック方式に比べて、以下に示す点が大幅に改善される。情報サービスのプロバイダ側/ユーザ側とも暗号化/復号化処理が相対的に容易で短時間で処理できる。

【0024】情報サービスプロバイダ側は、マスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。

【0025】情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。

【0026】ICカードを用いた個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用することができる。

【0027】暗号化鍵情報の制御情報内に、機器情報や領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止できる。この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。

【0028】

【課題を解決するための手段】この発明の情報記録媒体は、暗号化されている暗号化情報と、この暗号化情報を

元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録されるにものにおいて、上記暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録される。

【0029】この発明の記録装置は、暗号化鍵原案情報と復号化する際の条件情報とを設定する設定手段と、この設定手段により設定された暗号化鍵原案情報と非暗号化された状態の条件情報とにより暗号化鍵情報を生成する第1の生成手段と、共通鍵情報を記録する記録手段と、上記第1の生成手段により生成された暗号化鍵情報を上記記録手段に記録されている共通鍵情報により復号化して鍵情報を生成する第2の生成手段と、暗号化する情報を入力する入力手段と、この入力手段により入力された暗号化する情報を上記第2の生成手段により生成された鍵情報により暗号化して暗号化情報を生成する第3の生成手段と、上記第1の生成手段により生成された条件情報を含む暗号化鍵情報と上記第3の生成手段により生成された暗号化情報とが対応した状態で情報記録媒体に記録する記録手段とからなる。

【0030】この発明の情報伝送システムは、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とが記録される情報記録媒体を有する第1の装置と、この第1の装置と通信回線を介して接続され、上記第1の装置の情報記録媒体からの暗号化情報と暗号化鍵情報とが伝送される第2の装置とからなるものにおいて、上記第1の装置の情報記録媒体に記録される暗号化鍵情報に、非暗号化された状態で上記暗号化情報を復号化する際の条件情報が記録され、上記第1の装置が、上記情報記録媒体に記録されている条件情報を含む暗号化鍵情報と暗号化情報とを上記第2の装置へ送信する送信手段からなり、上記第2の装置が、上記第1の装置からの条件情報と暗号化鍵情報と暗号化情報とを復号化の処理を行う処理媒体に出力する第1の出力手段と、上記処理媒体からの復号化された情報に応じて処理を実行する実行手段からなり、上記処理媒体が、上記第2の装置からの条件情報に基づいて復号化を許可するか否かを判断する判断手段と、この判断手段により復号化の許可を判断した際に、上記第2の装置からの暗号化鍵情報に基づいて暗号化情報を復号化する復号化手段と、この復号化手段により復号化された情報を上記第2の装置へ出力する第2の出力手段とからなる。

【0031】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する

生成手段と、上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段とからなる。

【0032】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱う携帯可能媒体において、第1の特定情報と共通鍵情報とが入力される入力部と、この入力部から入力される第1の特定情報と共通鍵情報とにより第2の特定情報を生成する第1の生成手段と、この第1の生成手段により生成される第2の特定情報を記録する記録手段と、この記録手段への記録後、上記入力部からの入力を禁止する禁止手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する第2の生成手段と、上記暗号化鍵情報を上記第2の生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段とからなる。

【0033】この発明の暗号解読装置は、暗号化されている暗号化情報と、この暗号化情報を復号化する際の条件情報を含み上記暗号化情報を元の情報に復号化するための鍵情報を暗号化した暗号化鍵情報とを扱うものにおいて、第1の特定情報と共通鍵情報とにより生成される第2の特定情報を記録している記録手段と、第1の特定情報を設定する設定手段と、この設定手段により設定される第1の特定情報と上記記録手段に記録されている第2の特定情報とにより上記共通鍵情報を生成する生成手段と、上記暗号化鍵情報を上記生成手段により生成される共通鍵情報により復号化して鍵情報を得る第1の復号化手段と、上記暗号化情報を上記第1の復号化手段により得られた鍵情報により復号化して暗号化前の情報を得る第2の復号化手段と、上記条件情報により復号化を許可するか否かを判断する判断手段と、この判断手段により判断結果に基づき、上記第1、第2の復号化手段による復号化の実行を制御する制御手段とからなる。

#### 【0034】

【発明の実施の形態】以下、図面を参照してこの発明の実施例に係る光ディスク再生装置を説明する。以下、この発明の第1の実施の形態について図面を参照して説明する。

【0035】図1は、この発明の情報伝送システムを示すものである。この情報伝送システムは、クライアントマシン1と、このクライアントマシン1と通信回線2を介して接続されるホストサーバ3と、クライアントマシン1に装填あるいは内蔵される暗号解読部としてのIC

カード4により構成されている。

【0036】すなわち、クライアントマシン1からの所定のデータとしてたとえばワープロソフト等のプログラムの転送要求がホストサーバ3へ送信される。この送信に応じて、ホストサーバ3がその転送要求に応じて、後述する記録部としてのハードディスク装置(HDD)29に記録されている暗号化されているワープロソフト等のプログラム(暗号化情報)をその暗号化情報に対応する暗号化鍵情報(復号化するための情報で暗号化されている)とともに、転送要求のあったクライアントマシン1に返送される。この返送に応じて、クライアントマシン1はICカード4を用いて暗号化情報を暗号化鍵情報により復号化(解読)し、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになっていく。

【0037】上記ハードディスク装置(HDD)29には、ユーザに提供するサービス情報毎に記録されている。このサービス情報としては、単なる特定データだけでなく、例えばプログラミング(java)言語などで記述されたアプリケーション用の小単位の機能プログラムを含む。

【0038】上記ハードディスク装置(HDD)29に記録されている1つのサービス情報の構造例を、図2を用いて説明する。すなわち、暗号化情報としての暗号化されているワープロソフト等のプログラム(ユーザが使用する情報)40とこの暗号化情報40を復号化(解読)する鍵情報が暗号化されている暗号化鍵情報41とからなる情報が記録されている。

【0039】暗号化鍵情報41内には、その一部に非暗号化された形で(直接読める形で)制御情報42が含まれている。制御情報42は、対応する暗号化情報40を復号化(解読)する際の条件情報である。

【0040】制御情報42は、図3に示すように、1ビットのコピー許可コード43、4ビットのドライブコード44、32ビットのアドレスコード45、3ビットのリージョンコード46、16ビットの情報作成日情報47、7ビットの情報作成後のコピー禁止期間情報48、24ビットの特定パスワード情報49、32ビットの特定ユーザ/組織情報50からなる119ビット構成となっている。

【0041】ドライブコード44、アドレスコード45は、機器情報51と呼んでいる。リージョンコード46は、領域情報と呼んでいる。情報作成日情報47、コピー禁止期間情報48は、時間的情報52と呼んでいる。特定パスワード情報49、特定ユーザ/組織情報50は、ユーザ限定情報53と呼んでいる。

【0042】コピー許可コード43は、コピーの許可、不許可を示すものであり、“1”の時はコピー許可を示し、“0”の時はコピー不許可を示している。ドライブコード44は、情報伝送経路や使用ドライブを示してい

る。

【0043】“1H（ヘキサ：16進法）”の時、情報伝送経路がISDN（LANネットワーク）10MHz対応を示している。“2H”の時、情報伝送経路がISDN（LANネットワーク）100MHz対応を示している。

【0044】“3H”の時、情報伝送経路がISDN（LANネットワーク）500MHz対応を示している。“4H”の時、情報伝送経路が一般有線電話線（モデム利用）を示している。

【0045】“5H”の時、情報伝送経路が地上波（多重TVチャンネル）を示している。“6H”の時、情報伝送経路が衛星放送を示している。“7H”の時、情報伝送経路が無線通信（PHS、携帯電話ネットワーク）を示している。

【0046】“8H”の時、情報伝送経路が局所無線通信（家庭内通信、事業所内通信）を示している。“9H”の時、情報伝送経路がケーブルネットワーク、“AH”の時、情報伝送経路（使用ドライブ）がFDDを示している。

【0047】“CH”の時、情報伝送経路（使用ドライブ）が（起動時のオペレーションシステムが記録されている）ブートHDDを示している。“DH”の時、情報伝送経路（使用ドライブ）がMO、PDなど光ディスクを示している。

【0048】“EH”の時、情報伝送経路（使用ドライブ）がCD-ROM、CD-Rを示している。“FH”の時、情報伝送経路（使用ドライブ）がDVDDVideo、DVD-ROMを示している。

【0049】“OH”の時、情報伝送経路（使用ドライブ）がDVD-RAMあるはDVD-Rを示している。アドレスコード45は、送信先や送信元を識別するためのアドレスデータ（IPアドレス）を示し、たとえばネットワークアドレスとホストアドレスから構成されている。このアドレスコード45は、情報伝達がISDN（LANネットワーク）の場合に付与されている。

【0050】リージョンコード46は、地球上の地域を8地域に分け、各地域毎に16進法で1Hから8Hの番号を付与したものである。リージョンコード46は、領域情報に対応している。

【0051】情報作成日情報47は、情報作成日を示すものであり、7ビットの年情報、4ビットの月情報、5ビットの日情報で記述されている。コピー禁止期間情報48は、コピー禁止期間つまりコピー不許可期限を示すものであり、コピー許可コードが“0”のコピー不許可の場合に、付与されるものである。このコピー禁止期間情報48は、最高10年7か月＝127ヶ月まで記述でき、“0000000”の場合には永久にコピー禁止を示している。

【0052】特定パスワード情報49は、アルファベッ

トと数字の4文字分で示される特定のパスワードを示すものであり、1文字分ずつに36種類の文字が選択できるようにになっている。この場合、1文字ずつが6ビットのコードで記述されている。

【0053】特定ユーザ／組織情報50は、特定ユーザや組織を示すものである。上記制御情報42の内容は、情報伝送システムで取り扱う情報内容（コンテンツ）により簡素化するようにしても良い。たとえば、もっとも簡易的なシステムとしては、制御情報42が1ビットのコピー許可コード43のみから構成されるものであっても良い。

【0054】上記した図3に示す構造を有する制御情報42が、そのまま図2に示す暗号化鍵情報41内に嵌め込まれる。この暗号化鍵情報41のサイズは、制御情報42のサイズより大きいものであり、ハッカーによる暗号化鍵情報41の読取を防止するためには、最低でも暗号化鍵情報41のサイズは、制御情報42の2倍は必要で、実際には3倍以上が望ましい。

【0055】したがって、上記した制御情報42が119ビット構成の場合、暗号化鍵情報41は最低でも238ビット、通常でも357ビット以上は必要となる。また、1ビットのコピー許可コード43のみから制御情報42が構成されている場合、暗号化鍵情報41は最低でも2ビット、通常でも3ビット以上は必要となる。

【0056】ICカード4は、図4に示すように、後述するICカードリーダー・ライター13に接続されるコネクタ部としての電極部5と、ユーザパスワード入力端子用穴6と、マスター鍵入力端子用穴7とを有している。ユーザパスワード入力端子用穴6内にユーザパスワード入力端子6aがあり、マスター鍵入力端子用穴7内にマスター鍵入力端子7aがある。

【0057】ユーザパスワード入力端子用穴6と、マスター鍵入力端子用穴7とは、ICカード4の発行装置により発行される際に、ユーザパスワード（第1の特定情報）とマスター鍵情報（共通鍵情報）の入力によりユーザ対応鍵情報（第2の特定情報）が生成されて、後述するEEPROM34に記録された後、樹脂封入等で埋め込まれるようになっている。これにより、後からユーザ対応鍵情報が変更できない、つまり不正改ざんできないようにしている。

【0058】すなわち、ユーザ、つまりICカード4の発行者であるプロバイダーにより入力される、第2の特定情報としてのユーザパスワードとマスター鍵の入力により、第1の特定情報としてのユーザ対応鍵情報を形成した後、改ざん防止のため、その入力部（入力端子）への外部からの入力経路を遮断している。

【0059】また、ユーザパスワード入力端子用穴6、マスター鍵入力端子用穴7が埋められる代りに、ユーザパスワード入力端子6a、マスター鍵入力端子7a自体を取り外したり、あるいはそれらの電極部分を取り外し



たりすることにより、後からユーザ対応鍵情報を変更できないようにしても良い。この場合、入力端子の代りにリード線を用い、発行時にリード線を引抜くことにより、取り外すようにしても良い。

【0060】クライアントマシン1は、パソコン等の情報処理機器であり、図5に示すように、クライアントマシン1の全体を制御するCPU10、制御プログラムが記録されているROM11、データ記録用のRAM12、上記ICカード4との間でデータのやり取りを行うICカードリーダー・ライタ13、表示部14、入力部としてのキーボード15、記録部（情報記録媒体）としてのハードディスク装置（HDD）16、光ディスク17aが装填される記録部としての光ディスク装置17、および上記通信回線2を介してホストサーバ3と接続される通信インターフェース18により構成されている。

【0061】ハードディスク装置（HDD）16、光ディスク装置17は、オプションにて後から接続できるものである。ホストサーバ3は、図6に示すように、ホストサーバ3の全体を制御するCPU20、制御プログラムが記録されているROM21、データ記録用のRAM22、あらかじめマスター鍵情報が記録されているEEPROM23、生情報を鍵情報により暗号化情報40への暗号化を行う暗号器24、暗号化鍵情報41をマスター鍵情報により鍵情報への復号化を行う復号器25、暗号化鍵情報41を生成する鍵情報合成器26、表示部としてのCRTディスプレイ27、ユーザパスワードをユーザが入力する入力部としてのキーボード28、暗号化されているワープロソフト等のプログラム（暗号化情報）とこの暗号化情報に対応する暗号化鍵情報とからなる情報が記録されている記録部（情報記録媒体）としてのハードディスク装置（HDD）29、上記通信回線2を介してクライアントマシン1と接続される通信インターフェース30により構成されている。

【0062】上記ハードディスク装置（HDD）29の代りに光ディスク装置を用いても良い。さらに、大容量の記録部とする場合には、RAID（redundant arrays inexpensive disk）等のディスクアレイにより構成されるようにしても良い。

【0063】上記鍵情報合成器26は、暫定的に暗号化鍵としての暗号化鍵原案情報と制御情報42との合成を行い、合成結果として暗号化鍵情報41を生成するものであり、例えば図7に示すように2つのシフトレジスタ26a、26bにより構成されている。

【0064】これにより、シフトレジスタ26a、26bは、供給される暗号化鍵原案情報を順次出力し、CPU20からのロード信号が供給された際に、制御情報41をロードすることにより、その暗号化鍵原案情報に制御情報41を嵌め込んで出力するようになっている。この際、CPU20はRAM22から読出す暗号化鍵原案情報のアドレスに基づいてロード信号が出力されるよう

になっている。

【0065】上記暗号器24、復号器25は、それぞれ図8に示すように、7個のシフトレジスタ60a～60gと3個の排他的論理和演算を行う演算器61a～61cにより構成されている。

【0066】暗号器24の場合には、たとえば、乱数としての鍵情報「1010010001011」がシフトレジスタ60a～60gに供給され、生情報「1110001110001」が演算器61cに供給された場合、暗号化結果として、演算器61cから暗号化情報「1011100000101」が出力される。

【0067】復号器25の場合には、たとえば、乱数としてのマスター鍵情報「110100000110」がシフトレジスタ60a～60gに供給され、暗号化鍵情報「1000011100101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての鍵情報「1010010001011」が出力される。

【0068】なお、ユーザパスワードを入力する入力部としてキーボード28を用いているが、ユーザパスワードの代わりに声紋を用い、入力部としてマイクと声紋特徴検出器とを用いるようにしても良い。また、ユーザパスワードの代わりに顔情報を用い、入力部としてCCD等からなる顔画像読取部と顔情報特徴抽出器とを用いるようにしても良い。また、ユーザパスワードのキー入力の代わりにパスワードの音声認識を用い、入力部としてマイクと音声認識装置とを用いるようにしても良い。また、ユーザパスワードの代わりに指紋を用い、入力部としてCCD等からなる指紋読取部と画像特徴抽出器とを用いるようにしても良い。また、ユーザパスワードの代わりに指情報を用い、入力部として電極アレイによる各点での指表面抵抗値測定装置と指情報特徴抽出装置とを用いるようにしても良い。

【0069】上記ICカード4は、図9に示すように、ICカード4の全体を制御するCPU31、制御プログラムが記録されているROM32、データ記録用のRAM33、ユーザ対応鍵情報、ユーザパスワード、ユーザID等が記録されるEEPROM34、ユーザ対応鍵情報を生成するユーザ対応鍵情報生成器35、マスター鍵情報を生成するマスター鍵生成器36、暗号化鍵情報41をマスター鍵情報により鍵情報への復号化を行う復号器37、暗号化情報40を鍵情報により生情報への復号化を行う復号器38、インターフェース39、コネクタ部5、ユーザパスワードが入力されるユーザパスワード入力端子6a、マスター鍵情報が入力されるマスター鍵入力端子7aにより構成されている。

【0070】上記ICカード4は、セキュリティの確保のためユーザ個々人に認証用ICカード20を持たせており、このICカード20内に全ての復号化回路が内蔵されている。この方式ではマスター鍵情報6や鍵情報3



がICの外に出ることは無く、ハッカーによる不正を防止している。従って図1に示した情報伝送システムでは復号化回路が内蔵されているICカード20が暗号解読装置であり、情報伝送システム全体から見ると暗号解読部に相当する。

【0071】ユーザ対応鍵情報生成器35は、排他的論理和演算を行う演算器で構成され、ユーザパスワード入力端子6aから入力されるユーザパスワードとマスター鍵入力端子7aから入力されるマスター鍵情報の排他的論理和演算を行うことにより、演算結果としてユーザ対応鍵情報を生成するものである。

【0072】たとえば、ユーザパスワード「1100」とマスター鍵情報「1010」の演算により、ユーザ対応鍵情報「1001」を生成する。マスター鍵生成器36は、排他的論理和演算を行う演算器で構成され、EEPROM34から読出されたユーザ対応鍵情報と外部から供給されるユーザパスワードの排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成するものである。

【0073】たとえば、ユーザ対応鍵情報「1001」とユーザパスワード「1100」の演算により、マスター鍵情報「1010」を生成する。上記復号器37、38は、それぞれ図8に示すように、7個のシフトレジスタ60a~60gと3個の排他的論理和演算を行う演算器61a~61cからなる乱数発生器により構成されている。これにより、シフトレジスタ60a~60gにロードされた情報に対して、演算器61cに逐次供給される情報により演算を行うようになっている。

【0074】復号器37の場合には、たとえば、乱数としてのマスター鍵情報「110100000110」がシフトレジスタ60a~60gに供給され、暗号化鍵情報「1000011100101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての鍵情報「1010010001011」が出力される。

【0075】復号器38の場合には、たとえば、乱数としての鍵情報「1010010001011」がシフトレジスタ60a~60gに供給され、暗号化情報「1011100000101」が演算器61cに供給された場合、復号化結果として、演算器61cから復号化情報としての生情報「1110001110001」が出力される。

【0076】次に、ホストサーバ3によるハードディスク装置(HDD)29への上述した(ユーザに提供する)サービス情報の記録方法について、図10に示すフローチャートと、図11の暗号化鍵情報41と暗号化情報40の生成過程を示す図を参照しつつ説明する。

【0077】たとえば今、ホストサーバ3のプロバイダ(ユーザに対するサービス情報を提供する)がCRTディスプレイ27とキーボード28からなるユーザインタ

ーフェースを用いて、例えばプログラミング(java)言語などで記述されたアプリケーション用小単位の機能プログラムとしての生情報を入力する(ST1)。この生情報は、CPU20によりRAM22に記録される(ST2)。

【0078】さらに、ホストサーバ3のプロバイダは、ユーザインターフェースを用いて、上述した図7に示すようなコード許可コード43等からなる制御情報42の内容を入力する(ST3)。この制御情報42は、CPU20によりRAM22に記録される(ST4)。

【0079】さらに、ホストサーバ3のプロバイダは、ユーザインターフェースを用いて、暫定的に暗号化鍵としての暗号化原案情報を入力する(ST5)。この暗号化原案情報は、CPU20によりRAM22に記録される(ST6)。

【0080】そして、CPU20はRAM22に記録されている暗号化原案情報と制御情報42とを読み出し、鍵情報合成器26に出力することにより、鍵情報合成器26で暗号化原案情報と制御情報42との合成処理を行わせ、暗号化鍵情報41を生成する(ST7)。ついで、CPU20はこの生成された暗号化鍵情報41をRAM22に記録するとともに、ハードディスク装置(HDD)29へ記録する(ST8)。

【0081】ついで、CPU20はRAM22に記録されている上記生成された暗号化鍵情報41とEEPROM23に記録されているマスター鍵情報とを読み出し、復号器25に出力することにより、復号器25で暗号化鍵情報41をマスター鍵情報により復号化(解読)する処理を行わせ、鍵情報を生成する(ST9)。ついで、CPU20はこの生成された鍵情報をRAM22に記録する(ST10)。

【0082】ついで、CPU20はRAM22に記録されている生情報と上記生成された鍵情報とを読み出し、暗号器24に出力することにより、暗号器24で生情報を鍵情報により暗号化する処理を行わせ、暗号化情報40を生成する(ST11)。ついで、CPU20はこの生成された暗号化情報40を上記暗号化鍵情報41に対応させてハードディスク装置(HDD)29へ記録する(ST12)。

【0083】この場合、始めに暗号化鍵情報41を先に作り、そのあと復号器を通して初めて鍵情報を生成し、この生成した鍵情報を用いて暗号器でユーザに供給するサービス情報である暗号化情報40を生成し、この生成された暗号化情報40を上記暗号化鍵情報40とともにHDD29に記録されるようにしたものである。

【0084】次に、情報サービスプロバイダによる上記ICカード4の発行処理、つまりユーザ対応鍵情報のICカード4内への登録方法について、図12に示すフローチャートを参照しつつ説明する。基本的にはICカード4がユーザの手元に届く前に情報サービスプロバイダ

が設定を行う。

【0085】このICカード4を発行する発行機は、上記ICカード4のコネクト部5とデータのやり取りが行えるとともに、ユーザパスワード入力端子6aとマスター鍵入力端子7aを介して入力が行えるカードリーダー・ライタと、表示部と入力部からなるユーザインターフェースと、発行処理を制御する制御部から構成されている。

【0086】すなわち、情報サービスプロバイダは何も記録がなされていないICカード4を上記発行機に挿入する(ST21)。これにより、発行機のカードリーダー・ライタとICカード4のコネクト部5、ユーザパスワード入力端子6a、マスター鍵入力端子7aとが接続される(ST22)。

【0087】さらに、情報サービスプロバイダはユーザインターフェースによりICカードの発行を指示するとともに、ユーザとの契約時に情報サービスプロバイダが決めたユーザパスワードと情報サービスプロバイダのみが知っているマスター鍵情報とを入力する(ST23)。これにより、ICカードリーダー・ライタ13およびユーザパスワード入力端子6aとマスター鍵入力端子7aを介して、ユーザパスワードとマスター鍵情報とがユーザ対応鍵情報生成器35に供給される(ST24)。すると、ユーザ対応鍵情報生成器35はそれらの情報のビット単位の排他的論理和演算を行うことによりユーザ対応鍵情報を生成し、EEPROM34に出力する(ST25)。これにより、EEPROM34にユーザ対応鍵情報が記録される(ST26)。

【0088】また、ユーザ対応鍵情報が記録された後、情報サービスプロバイダはユーザとの契約時に決められたユーザパスワードとユーザIDとを入力する。これにより、CPU10は、ユーザパスワードとユーザIDとをICカードリーダー・ライタ13、コネクト部5、およびインターフェース39を介してCPU31に出力する。CPU31は、供給されるユーザパスワードとユーザIDとをEEPROM34に記録する。

【0089】上記ユーザ対応鍵情報等が記録された後、上記発行機からICカード4が発行される。この発行されたICカード4に対して、ユーザパスワード入力端子用穴6とマスター鍵入力端子用穴7が、プロバイダにより樹脂封入等で埋めこまれる。これにより、ユーザ対応鍵情報生成器35への外部からの入力経路を遮断することができ、後からユーザ対応鍵情報が変更できない、つまり不正改ざんを防止できる。

【0090】次に、クライアントマシン1における立上げ処理により、ホストサーバ3に対してワープロソフト等のプログラムの転送要求を行い、この要求に応じて得られる暗号化されている情報をICカード4により解読して、機能プログラムとして設定する処理について、図13に示すフローチャートを参照しつつ説明する。

【0091】まず、クライアントマシン1の図示しない電源をオンし、クライアントマシン1を立上げる(ST31)。すると、クライアントマシン1は、ホストサーバ3とのやり取りにより、特定のグループ(課金システム等)に欲しいデータがあるかを確認する(ST32)。たとえば、情報サービスとしてのワープロソフト等のプログラムのリクエストを行う。この確認(リクエスト)が指示された際、CPU10は上記データの呼び出しが可能な(解読が行える)ICカード4の挿入を表示部14により案内する(ST33)。この案内に応じて、ユーザは対応するICカード4を挿入する(ST34)。

【0092】ついで、CPU10はユーザIDとユーザパスワードの入力を表示部14により案内する(ST35)。この案内に応じて、ユーザはユーザIDとユーザパスワードを入力する(ST36)。

【0093】この入力されたユーザIDとユーザパスワードは、CPU10によりICカードリーダー・ライタ13、コネクト部5、インターフェース39を介してICカード4内のCPU31に供給される(ST37)。これにより、CPU31は供給されたユーザIDとユーザパスワードとEEPROM23に事前に記録されているユーザIDとユーザパスワードとをそれぞれ比較し、一致するかどうかを判断し(ST38)、一致時、ユーザIDをクライアントマシン1に通知し(ST39)、不一致時、不正と見なし動作を停止し、NG信号をクライアントマシン1に通知する(ST40)。

【0094】上記ステップ38による判断結果の一致時に、ステップ39の処理と並行して、CPU31は上記ユーザパスワードとEEPROM34に事前に記録されているユーザ対応鍵情報とをマスター鍵生成器36により排他的論理和演算を行い、演算結果としてマスター鍵情報を生成し、RAM33に記録しておく(ST41)。

【0095】上記ステップ39によりユーザIDが通知されたクライアントマシン1は、上述したユーザによる情報サービスとしてのワープロソフト等のプログラムのリクエストに基づいた情報サービス要求とICカード4から得られたユーザIDとにクライアントマシン1のIPアドレスを付与してホストサーバ3に送信する(ST42)。このホストサーバ3はその転送要求に応じて、ユーザIDを認証後、ハードディスク装置(HDD)29に暗号化されて記録されている情報サービスとしてのワープロソフト等のプログラム(暗号化情報40)とその暗号化情報に対応する暗号化鍵情報41(復号化するための情報で暗号化されている)とに送信元と送信先のアドレスが入っているIPアドレスを付与した通信パケットに入れて、転送要求のあったクライアントマシン1に返送する(ST43)。この際、情報サービスの送信として、上記ユーザIDのユーザに対する課金の内容が

図示しない記録部に記録される。

【0096】上記返送に応じて、クライアントマシン1はICカード4を用いて暗号化情報40を暗号化鍵情報41とこの暗号化鍵情報41内の制御情報42により復号化（解読）し（ST44）、この復号化されたワープロソフト等のプログラムを用いて処理が行えるようになる（ST45）。

【0097】上記暗号化情報40の復号化処理について、図14に示すフローチャートを参照しつつ説明する。すなわち、クライアントマシン1のCPU10は、受信した通信パケット内のIPアドレスによりホストサーバ3が設置されている地域のリージョンコードを判断し、その送信元のIPアドレスと判断したリージョンコードとからなり、もし通信回線2が10MHzのLANネットワークの場合には上述したようにドライブコード44の値である「1H」も付加したクライアントマシン生成情報を作成し、ICカード4へ送る（ST51）。

【0098】これにより、ICカード4のCPU31は供給されるクライアントマシン生成情報をRAM33に記録する（ST52）。また、その情報の供給と並行して、CPU31は上記一致が判定されているユーザパスワードとEEPROM34に事前に記録されているユーザ対応鍵情報とをマスター鍵生成器36により排他的論理和演算を行うことにより、演算結果としてマスター鍵情報を生成し、RAM33に記録する（ST53）。

【0099】以上の準備が整った段階で、ICカード4のCPU31はコピー許可コード43の送信要求をクライアントマシン1のCPU10へ送信する（ST54）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41内に埋め込まれている制御情報42の中からコピー許可コード43を取出し、ICカード4のCPU31へ送信する（ST55）。

【0100】これにより、ICカード4のCPU31はコピー許可コード43が“1”か“0”かで、コピー許可かコピー不許可を判断する（ST56）。この判断の結果、コピー許可が判断された場合、CPU31は暗号化情報40等の出所がHDD16や光ディスク装置17のディスクに複製されたものだとしても無条件に受け、後段のステップ61の復号化作業へと進む。

【0101】上記ステップ56の判断の結果、コピー不許可が判断された場合、暗号化情報40等の出所を確認する必要があるため、CPU31はドライブコード44、アドレスコード45、リージョンコード46の送信要求をクライアントマシン1のCPU10へ送信する（ST57）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41内に埋め込まれている制御情報42の中からドライブコード44、アドレスコード45、リージョンコード46を取出し、ICカード4のCPU31へ送信する（ST58）。

【0102】これにより、ICカード4のCPU31は

クライアントマシン1から供給されるドライブコード44、アドレスコード45、リージョンコード46と、RAM33に記録されているクライアントマシン生成情報との一致を確認する（ST59）。

【0103】すなわち、暗号化情報等の出所が10MHzのISDNであればクライアントマシン生成情報内のドライブコードは“1H”となり、制御情報42のドライブコード44の“1H”と一致し、暗号化情報等の出所が正しいものと判断される。

【0104】また、暗号化情報等の出所がHDD16から再生されている場合にはクライアントマシン生成情報内のドライブコードは“CH”となり、制御情報42のドライブコード44の“1H”と一致しないため、暗号化情報等の出所が正しくない、つまり不正コピーした情報と判断される。

【0105】また、クライアントマシン生成情報内の送信元のIPアドレスと制御情報42のアドレスコード45とが一致しているか否かにより、暗号化情報等がオリジナルなものか海賊版として不正に商業用にコピーしたものなのかが判断される。

【0106】上記ステップ59により、不一致が判断された際、CPU31は、不正と見なし動作を停止し、NG信号をクライアントマシン1に通知する（ST60）。上記ステップ59により、一致が判断された際（暗号化情報等がオリジナルなものとして判断された際）、あるいは上記ステップ56によりコピー許可が判断された際、CPU31は、復号化の許可を判断し、復号化作業を開始を判断し、暗号化鍵情報41の送信要求をクライアントマシン1のCPU10へ送信する（ST61）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化鍵情報41をICカード4へ送信する（ST62）。

【0107】これにより、ICカード4のCPU31は復号器37によりクライアントマシン1から供給される暗号化鍵情報41をRAM33に記録されているマスター鍵情報により復号化（解読）する処理を行わせ、鍵情報を生成し、RAM33に記録する（ST63）。

【0108】ついで、CPU31は暗号化情報40の送信要求をクライアントマシン1のCPU10へ送信する（ST64）。この送信要求に応じて、クライアントマシン1のCPU10は、暗号化情報40をICカード4へ送信する（ST65）。

【0109】これにより、ICカード4のCPU31は復号器38によりクライアントマシン1から供給される暗号化情報42をRAM33に記録されている鍵情報により復号化（解読）する処理を行わせ、生情報を生成し、クライアントマシン1へ送信する（ST66）。

【0110】この生情報の送信に応じて、クライアントマシン1のCPU10は、送信されてきた生情報としてのワープロソフト等のプログラムをRAM22に記録す

る(ST67)。この結果、クライアントマシン1においてRAM22に記録されているワープロソフト等のプログラムを用いて処理を行うことができる。

【0111】上記のように、ユーザパスワードを用いてICカード4内でマスター鍵生成器により共通鍵であるマスター鍵情報をユーザには見えない場所で生成することができる。

【0112】また、ユーザ対応鍵情報をEEPROMにあらかじめ記録しておき、このユーザ対応鍵情報とユーザにより入力されるユーザパスワードとからマスター鍵生成器により共通鍵であるマスター鍵情報を生成し、この生成されたマスター鍵情報を用いて復号器により暗号化された情報を復号化できるようになっている。

【0113】上記したように、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。また、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0114】暗号化を技術的に見ると、データそのものを共通鍵で暗号化し、この共通鍵のみを公開鍵で再度暗号化するという従来のハイブリッド方式に比べ、2重に共通鍵を発行し、一方の共通鍵は暗号化して暗号化されたデータと一緒に情報伝達(暗号化された共通鍵の転送)し、他方の共通鍵はユーザからの特定情報を用いてICカード4内で復号化するものである。このため、伝達経路途中およびユーザ自身のどちらにも共通鍵が見えることがない。

【0115】したがって、共通鍵方式の欠点に対して、

1. 鍵の転送中の第三者による不正コピーされる危険性が少ない。
2. 鍵の管理が容易(ユーザはICカードを1枚持てば良い)。
3. 受信先での暗号データの改ざんが難しい。と大幅に改善されているだけで無く、アシンメトリック方式に比べて
4. 情報サービスプロバイダ側/ユーザ側とも、暗号化/復号化処理が相対的に容易で短時間で処理できる。
5. 情報サービスプロバイダ側はマスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。
6. 情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。
7. ICカードを用いた、個人認証用にユーザパスワードを入力するという、従来の認証手続だけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採

用することができる。

8. 暗号化鍵情報の制御情報内にドライブコードやアドレスコードが含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止できる。

【0116】この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。次に、第2の実施態様として、DVD-ROM等の光ディスク17aに第1の実施形態のホストサーバ3の記録部(HDD29)に記録したような暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41からなる情報(図2参照)が記録され、このDVD-ROM17aを第1の実施形態のクライアントマシン1の光ディスク装置(ROMドライブ)17に装填して再生する場合について説明する。

【0117】この場合、制御情報内のドライブコードとしてDVD-ROMを示す「FH」が記述され、時間情報として光ディスクの原盤が作成された時期を表す製造年月日が記述されている。

【0118】すなわち、第1の実施形態のようにホストサーバから暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41とIPアドレスからなる通信パッケージが送信される代わりに、光ディスク装置17に装填されたDVD-ROM17aから暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41とが再生される。以降の動作は、図13、図14に示すフローチャートの場合とほぼ同様に処理される。ただし、クライアントマシン生成情報内のドライブコードは「FH」となり、制御情報42のドライブコード44の「FH」と一致した際に、暗号化情報等の出所が正しいものと判断される。

【0119】また、光ディスク(DVD-ROM)17aに記録される暗号化情報としては、プログラム等の他にビデオデータ等他の情報であっても良い。また、図13、図14に示す動作の内、ユーザパスワードに関係した部分の処理(ステップ53)を行わないにしても良い。この場合、ICカード4にはユーザ対応鍵情報の代りにマスター鍵情報があらかじめEEPROM34に記録されている。

【0120】また、以下に示す光ディスク(DVD-ROM)17aの製造時に用いられ原盤70に、第1の実施例の図10～図12を用いて説明した暗号化情報40と制御情報42が嵌め込まれる暗号化鍵情報41のHDD29への記録と同様に、それらの情報が記録されることにより、光ディスク(DVD-ROM)17aが作成されるようになっている。

【0121】図15の(a)～(e)、図16の(f)から(k)を用いて上記光ディスク(DVD-ROM)17aの製造方法について説明する。表面精度を保証す

るため厚み0.5～30mmの強化ガラスで作られたガラス板71をスピンドルモータ72の上に乗せ(図15の(a))特定の回転数で回転させる。その上から有機溶媒に溶かされたフォトレジスト液をふりかけ、ガラス板71の回転による遠心力を利用してフォトレジスト液を均一に広げる。この塗布法をスピナーコーティング法と一般には呼ばれている。その後ガラス板71ごと60～300℃に高温放置して有機溶媒を蒸発させ、均一な厚みdrのフォトレジスト層73を形成する(図15の(b))。

【0122】後述する図16の(f)～図16の(i)の工程で転写効率が低下するが、仮に全行程での転写効率が100%だった場合にはこのフォトレジスト層73の厚みdrが最終的な情報記録媒体の記録膜84上でのビット深さまたはプリグループ深さになる。

【0123】その後、後述する原盤記録装置によりレーザ光75を対物レンズ76により集光させてフォトレジスト層73を断続的に露光し、露光部74を作成する(図15の(c))。全周に渡る露光が完了するとガラス板71ごと原盤記録装置から外し、図15の(d)に示すようにガラス板71を回転させながら現像液77を特定時間ふりかける。

【0124】すると図15の(e)のように露光部74が融けて穴落ち、段差drの微小凹凸が出来上がる。このようにして出来上がったガラス板71とフォトレジスト層73を光ディスクの原盤70と呼んでいる。このようにして作成した原盤70をスピンドルモータ72からはずし、Niによる無電解メッキ、電解メッキ(電鍍メッキ)により原盤70の凹凸形状のレプリカを取る。図16の(f)に示すようにこのようにして形成したレプリカをマスター板78と呼んでいる。マスター板78作成が完了するとアセトンなどの有機溶剤中に付けてフォトレジスト層73を溶かしてマスター板78を原盤70から剥離する。その後マスター板78を元に電解メッキ(電鍍メッキ)によりマザー板79を作成した後(図16の(g))、マザー板79をマスター板78から剥離する。再度マザー板79を元にして電解メッキ(電鍍メッキ)によりスタンパ80を作成する(図16の(h))。

【0125】一般に情報記録媒体の透明プラスチック基板83は“射出成形”と言う方法を用いて作成する。すなわち図16の(i)の用に金型A81、金型B82を配置し、その間の隙間に高温でどろどろに溶かした樹脂材(一般に使用材料としてポリカーボネート、PMMAやABSを用いる場合が多い)を押し込む。上記の工程で作成したスタンパ80は金型A81に取り付けて有るので、樹脂材が押し込まれた段階でスタンパ80の微小な凹凸形状が樹脂材に転写される。その後、数分放置して金型A81、金型B82ごと樹脂材を常温まで冷やし、樹脂材が冷えて固まった頃金型A81、金型B82

の間を広げてプラスチック基板83(上記の冷えて固まり・凹凸形状が転写された樹脂材をプラスチック基板83と呼んでいる)を取り出す。

【0126】このようにして得たプラスチック基板83を真空中に配置し、スパッタ蒸着や真空蒸着やイオンプレーティングなどの蒸着により記録膜84をプラスチック基板83上に形成し、図16の(j)のような構造を作る。このようにして作成した物を2枚記録膜84、86が内側になるように配置し、その間を記録膜84で充填して図16の(k)のような情報記録媒体を完成させる。

【0127】図15の(c)で示したフォトレジスト層73を局所的に露光させる原盤記録装置の構造を図17に示す。前述したようにガラス板71はスピンドルモータ72上で特定の回転数で回転する。レーザ光75は折り返しミラー88で反射後対物レンズ76によりフォトレジスト層73上に集光する。折り返しミラー88と対物レンズ76は可動部89として一体になってガラス板71の半径方向に移動する。この可動部89は送りモータ90と送りギヤ91により移動する。図示していないがガラス板76上の集光スポット位置を光学的にモニタするモニタ部分を持ち、このモニタ出力に応じてスピンドルモータ72の回転数が変化し、ガラス板71上での相対集光スポットの移動速度(線速)が常に一定になるように原盤記録制御部50がコントロールしている。

【0128】レーザ光源97から出たレーザ光75はE. O. 変調器94とA. O. 変調器93を通過後折り返しミラー88へ到達する。微小な凹凸ビット形状であるプリビット信号はプリビット信号発生器99の信号に応じて高速スイッチ96をオン/オフして可変電圧発生器95の電圧をE. O. 変調器94に対して印加したり、解放する。このE. O. 変調器94に対する印加電圧を変えるとE. O. 変調器94を通過するレーザ光量が変化する。このようにしてフォトレジスト層73へ到達するレーザ光量を変化させてフォトレジスト層73上の露光部74、非露光部を作る。

【0129】特定周波数発振器92により特定周波数の電圧をA. O. 変調器93に加えることによりA. O. 変調器93内の特定の距離的周期を持った定在波(A. O. 変調器93素子内の分子間の粗密波)が発生する。この定在波によりレーザ光75がブラッグ(Bragg)反射を受け、特定の方向に曲げられる。従ってこの定在波の距離的周期が変わることによりブラッグ(Bragg)条件が変わり、レーザ光75の曲がる角度も変化する。つまり特定周波数発振器92の出力周波数を変えることによりレーザ光75の進行方向が変化し、その結果フォトレジスト層73上で集光点位置が半径方向に移動する。

【0130】プリグループが特定周期蛇行する構造を有する情報記録媒体の場合にはウォーブル・グループ発生

器／グループ・ビット切替器98の出力に応じて特定の周期で周波数発振器92の周波数が変化している。またウォーブルビットの場合にはトラックピッチ（ランド・グループ間のピッチ）の半分だけ集光スポットがフォトレジスト層73上で半径方向にずれるように特定周波数発振器92の周波数を変化させる。

【0131】上記したように、暗号化情報を復号化するための一切の復号化手段を持たないROMドライブ17（クライアントマシン1）が単独に情報再生が可能か禁止かを判断できる。これにより、情報再生の禁止を検出した場合に、それ以降の復号化処理・再生処理を行うパソコン等の装置へ再生ならびに転送が禁止された情報を転送しないようにすることができる。

【0132】また、従来のものは、復号化後の鍵に制御情報を含ませた場合には、ROMドライブ内に鍵情報を復号化する復号化手段を持たせなければならず、コストも増加するし、従来のROMドライブとの互換性も取れなくなってしまうという欠点があるが、上記第2の実施態様では、そのような欠点を回避することができる。

【0133】また、他の実施態様として、図18に示すように、ホストサーバ101とユーザ用サーバ102とがそれぞれネットワーク103、104を介してネットワークコンピュータ105と接続されているネットワークシステムの場合について説明する。

【0134】たとえば、ホストサーバ101は、第1の実施形態のホストサーバ3と同じ構成であり、暗号化情報としての暗号化されているワープロソフト等のプログラム（ユーザが使用する情報）40と非暗号化された形で制御情報42が嵌め込まれその暗号化情報40を復号化（解読）する鍵情報が暗号化されている暗号化鍵情報41とからなる情報が記録されているHDD29を有している。

【0135】ネットワークコンピュータ105は、ネットワークコンピュータ105の全体を制御する制御部106、ホストサーバ101からの暗号化情報等を受信する受信部107、受信受信部107で受信した暗号化情報等の暗号を解読する暗号解読部108、暗号解読部108により解読された情報を記録するRAMメモリ109、制御部106による処理結果を暗号化する暗号器110、暗号器110により暗号化された処理結果をユーザ用サーバ102に情報を発信する発信部111により構成されている。上記暗号解読部108は、第1の実施形態のICカード4と同じ構成と機能を有しており、暗号器110も第1の実施形態の暗号器24と同じ構成と機能を有している。

【0136】これにより、ホストサーバ101からネットワーク102を経由して送られてきたJAVAなどで記述された小規模機能プログラムの暗号化情報等は受信部107で電気信号に変換され、そのまま暗号解読部108に入力され、復号化後の機能プログラムはRAMメ

モリ109に入力される。制御部106ではRAMメモリ109から機能プログラムを読み出しながら演算処理を実施する。処理後の結果は暗号器110で暗号化された後、発信部111からネットワーク103を経由してユーザ用サーバ102に送られる。

【0137】ネットワークコンピュータ105内の受信部107と発信部111を除く全回路はワンチップ化されているため復号化後の生信号は直接外に取り出せない構造になっており、いっそうセキュリティが強化されている。

【0138】また、他の実施態様として、放送衛星を利用した例を図19を用いて説明する。すなわち、キー局121から放送衛星122を経由して、第1の実施形態の図2に示すような暗号化情報等が送られてくる。情報再生装置123内の受信部124で電気信号に変換後、第1の実施形態のICカードにより形成される暗号解読部125で生信号に復号化され、表示部126で表示される。上述した各実施態様によれば、セキュリティ確保が必要であるかまたは著作権確保が必要な情報に関する不正な複製の防止を行うことができる。

【0139】

【発明の効果】以上詳述したように、この発明によれば、ホストサーバのユーザ要求毎の暗号化処理が不要となるため、低コストで情報配送が可能となる。この発明によれば、非常に容易に情報の不正コピーを発見することができ、セキュリティを大幅に向上させる事ができる。

【0140】この発明によれば、共通鍵方式の欠点に対して、鍵の転送中の第三者による不正コピーされる危険性が少なく、鍵の管理が容易で、受信先での暗号データの改ざんが難しいと言う点が大幅に改善される。

【0141】この発明によれば、アシンメトリック方式に比べて、以下に示す点が大幅に改善される。情報サービスのプロバイダ側／ユーザ側とも暗号化／復号化処理が相対的に容易で短時間で処理できる。

【0142】情報サービスプロバイダ側は、マスター鍵のみ設定すれば良く、ユーザ毎の管理センタへの公開鍵の問い合わせを行う必要がないので、ユーザへの情報提供作業が大幅に効率化できる。

【0143】情報サービスプロバイダ側は、事前に暗号化された情報をICカード側に記録しておき、それをそのまま配送できる。このため、ユーザの要求毎に暗号化して情報配送する従来の暗号化方式と比べると、情報サービスプロバイダ側の負担は大幅に改善される。

【0144】ICカードを用いた個人認証用にユーザパスワードを入力するという、従来の認証手続きだけで、復号化の準備が完了する。従って、セキュリティ確保のため、新たにユーザに負担を強いることなく、暗号化技術を採用することができる。

【0145】暗号化鍵情報の制御情報内に、機器情報や

領域情報が含まれているため、ユーザ側で暗号化された情報をそのままHDDや光ディスクにコピーし、不正使用をすることを防止できる。この結果、従来の暗号化技術の欠点をすべて改善し、情報送付元・受信先ともに処理を大幅に簡素化し、セキュリティ機能を強化することができる。

【図面の簡単な説明】

【図1】図1は、この発明の実施の形態を説明するための情報伝送システムの概略構成を示す図。

【図2】図2は、サービス情報の構造例を示す図。

【図3】図3は、制御情報の構成例を示す図。

【図4】図4は、図1のICカードの構成を示す斜視図。

【図5】図5は、図1のクライアントマシンの概略構成を示すブロック図。

【図6】図6は、図1のホストサーバの概略構成を示すブロック図。

【図7】図7は、図6の鍵情報合成器の概略構成を示すブロック図。

【図8】図8は、図6の暗号器、復号器の概略構成を示すブロック図。

【図9】図9は、図1のICカードの概略構成を示すブロック図。

【図10】図10は、サービス情報の記録方法を説明するためのフローチャート。

【図11】図11は、暗号化鍵情報と暗号化情報の生成過程を示す図。

【図12】図12は、ユーザ対応鍵情報のICカード内への登録方法を説明するためのフローチャート。

【図13】図13は、要求に応じて得られる暗号化されている情報をICカードにより解読して、機能プログラムとして設定する処理を説明するためのフローチャート。

【図14】図14は、暗号化情報の復号化処理を説明するためのフローチャート。

【図15】図15は、DVD-ROMの製造方法を説明するための図。

【図16】図16は、DVD-ROMの製造方法を説明するための図。

【図17】図17は、原盤記録装置の概略構成を説明するための図。

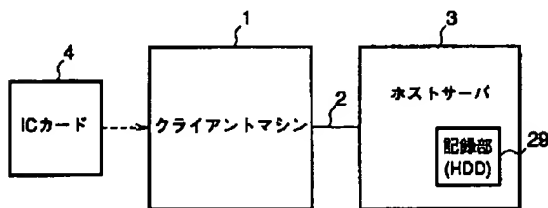
【図18】図18は、他の実施態様を説明するためのネットワークシステムの概略構成を示す図。

【図19】図19は、他の実施態様を説明するための放送衛星を利用した例を示す図。

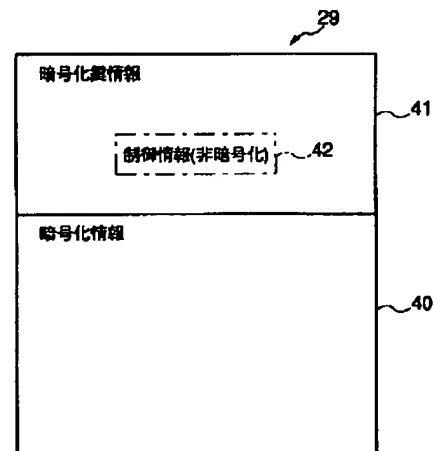
【符号の説明】

- 1…クライアントマシン
- 2…通信回線
- 3…ホストサーバ
- 4…ICカード
- 29…記録部(HDD)
- 40…暗号化情報
- 41…暗号化鍵情報
- 42…制御情報

【図1】

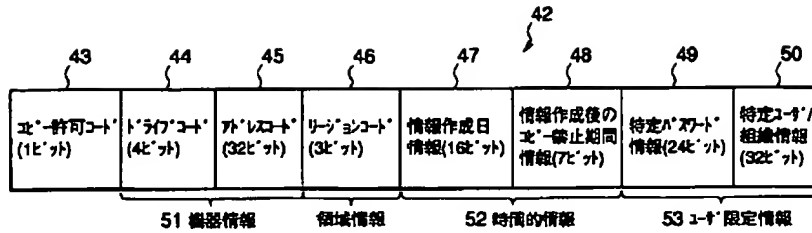


【図2】

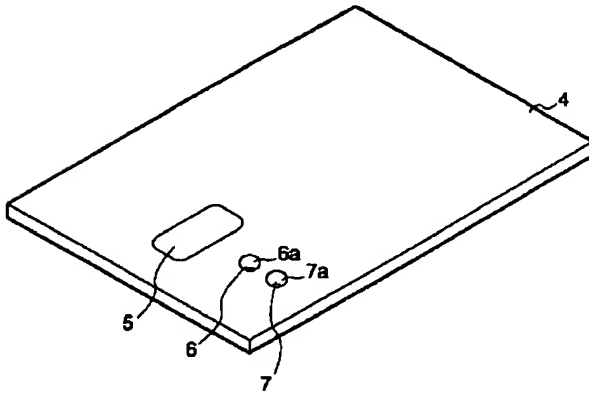




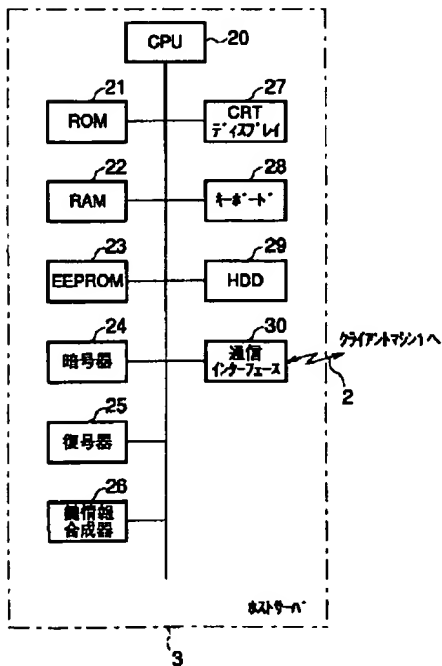
【図3】



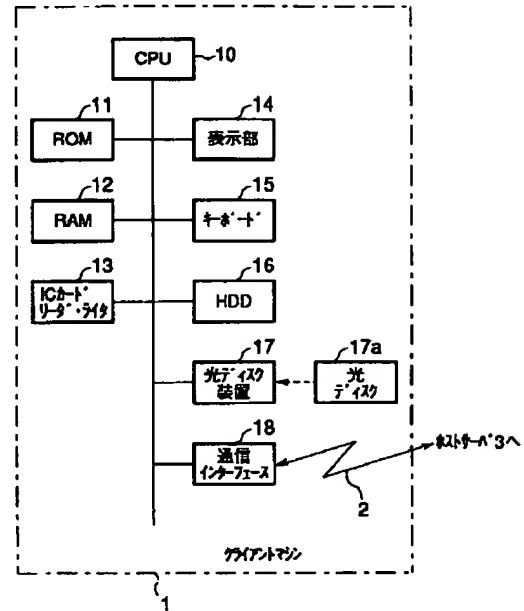
【図4】



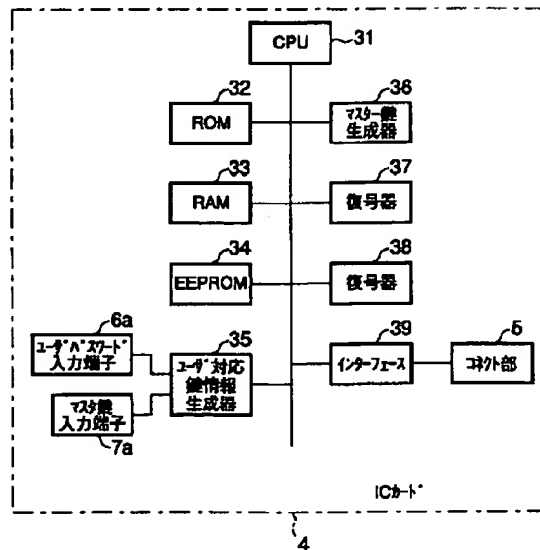
【図6】



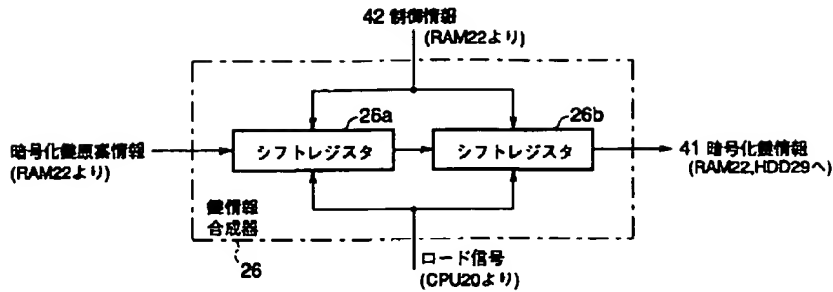
【図5】



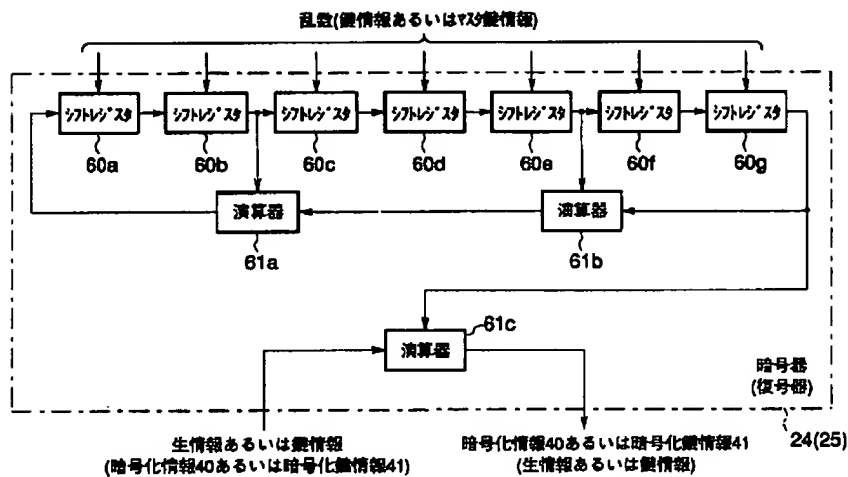
【図9】



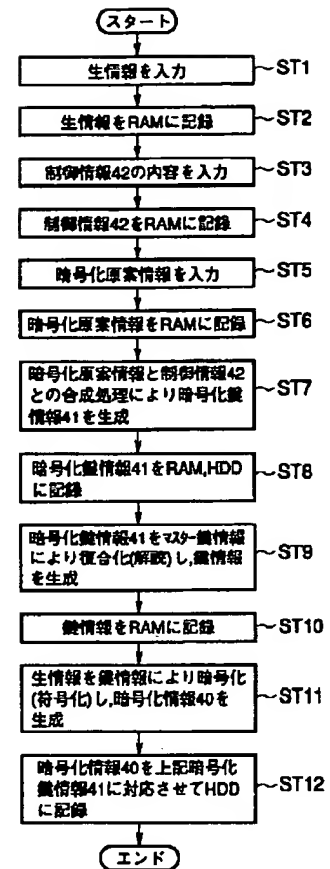
【図7】



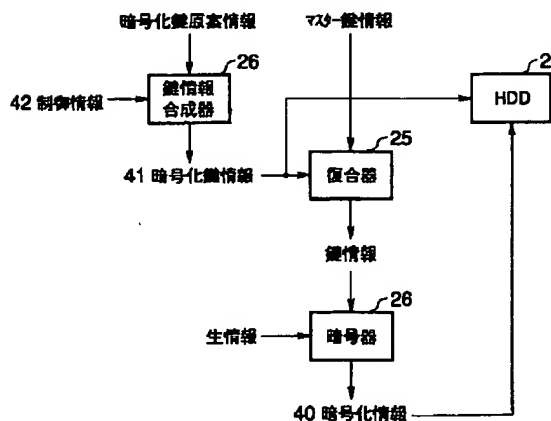
【図8】



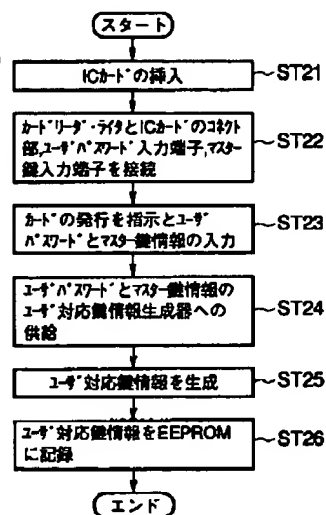
【図10】



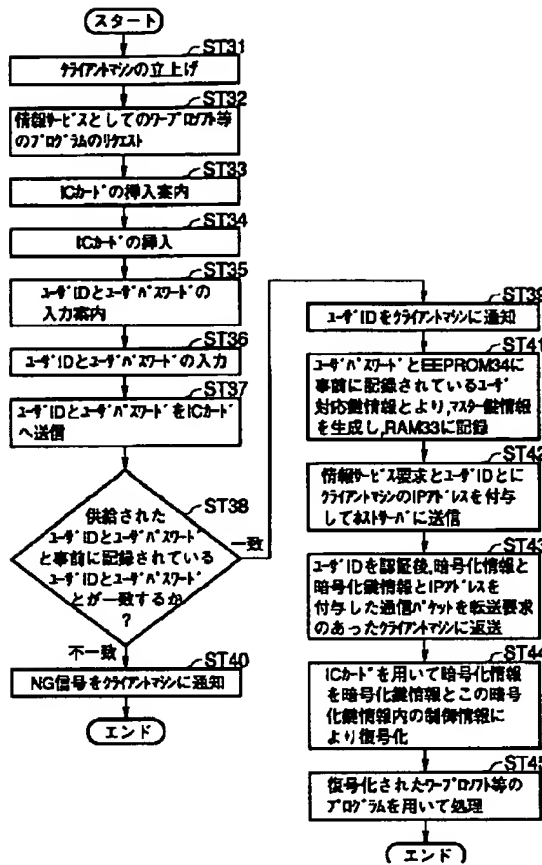
【図11】



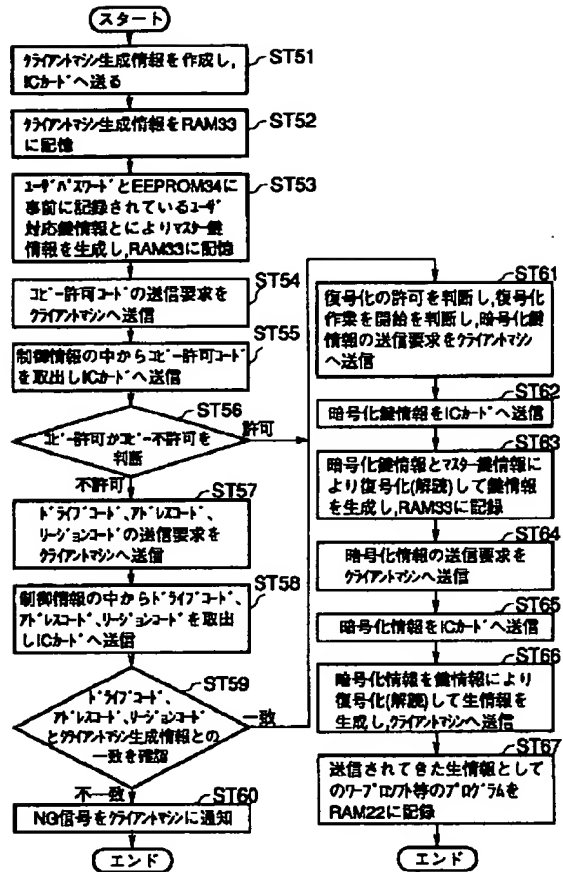
【図12】



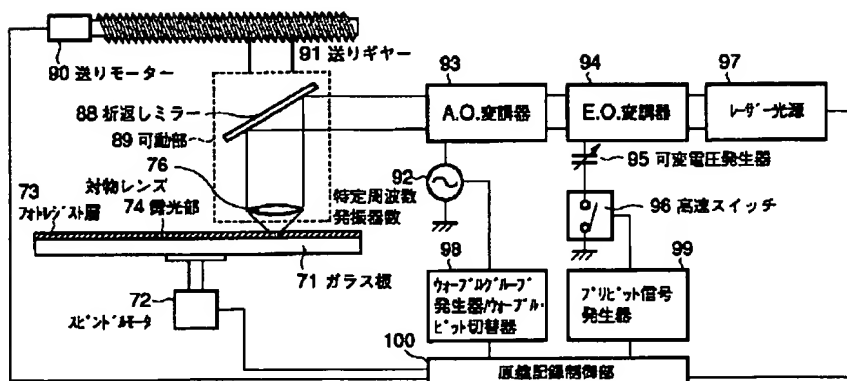
【図13】



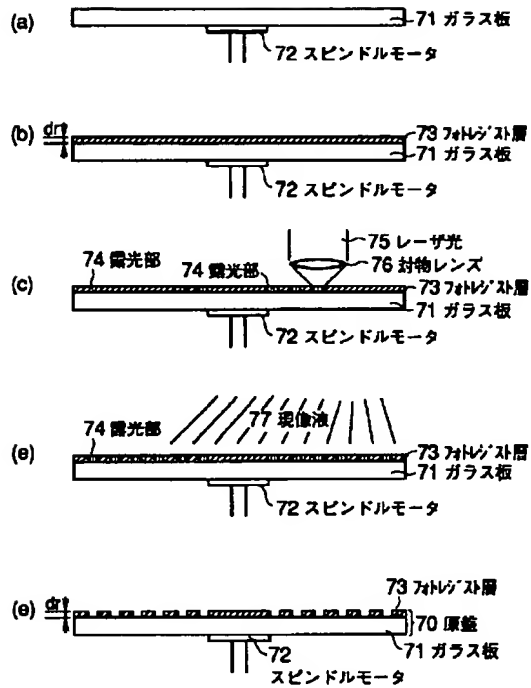
【図14】



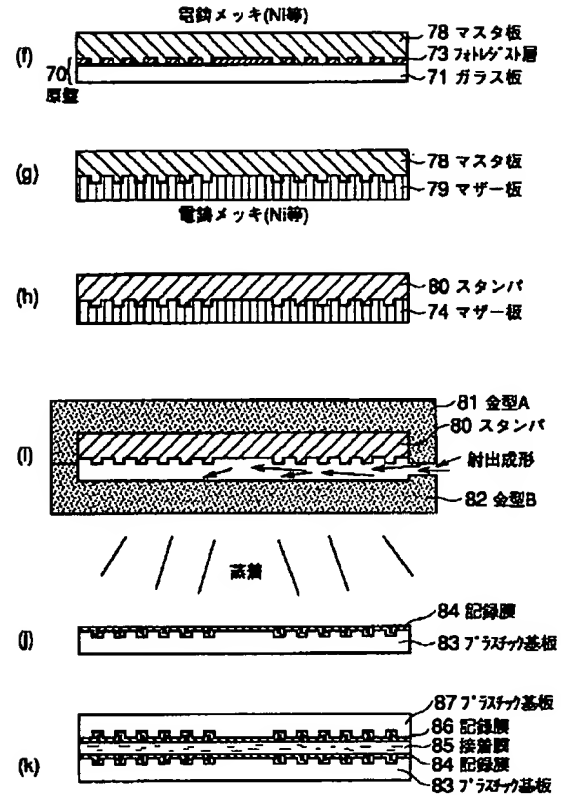
【図17】



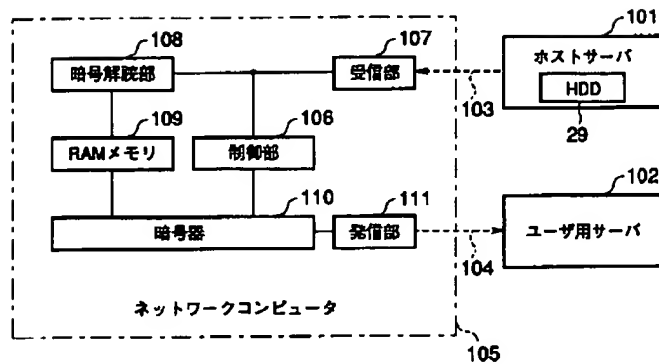
【図15】



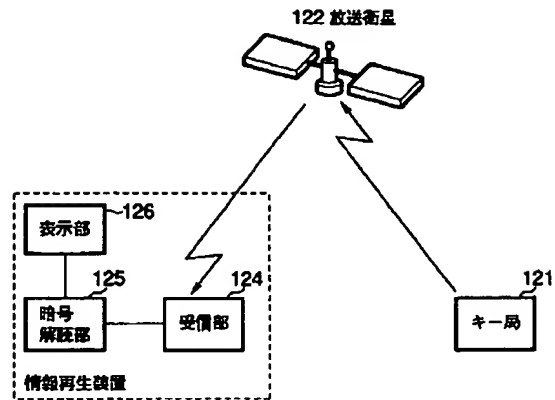
【図16】



【図18】



【図 19】




---

フロントページの続き

(51) Int. Cl. 6

G 1 1 B 20/10

H 0 4 L 9/32

識別記号

F I

G 0 6 K 19/00

H 0 4 L 9/00

R

6 7 1

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-283268

(43)Date of publication of application : 23.10.1998

---

(51)Int.Cl. G06F 12/14

G06K 17/00

G06K 19/10

G09C 1/00

G11B 20/10

H04L 9/32

---

(21)Application number : 10-023284 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 04.02.1998 (72)Inventor : YAMADA HISASHI  
ANDO HIDEO

---

(30)Priority

Priority number : 09 25303 Priority date : 07.02.1997 Priority country : JP

---

(54) INFORMATION RECORDING MEDIUM, RECORDER, INFORMATION

## TRANSMISSION SYSTEM, AND DECODING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent wrong copy of information requiring the protection of security or copyright at the time of decoding encryption information from an information recording medium.

SOLUTION: Enciphered encryption information 40 and encryption information 41 where information to decoder this encryption information 40 to original information is enciphered are recorded, and condition information for decoding of encryption information 40 is recorded in this encryption information 41 in the non-encryption state, and encryption information 41 and condition information 42 are used to decode encryption information 40 from the information recording medium 29 in an IC card 4.

---

### LEGAL STATUS

[Date of request for examination] 13.12.2000

[Date of sending the examiner's  
decision of rejection]

[Kind of final disposal of application  
other than the examiner's decision of  
rejection or application converted  
registration]

[Date of final disposal for application]

[Patent number] 3746146

[Date of registration] 02.12.2005

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]



[Date of extinction of right]

---

## CLAIMS

---

[Claim(s)]

[Claim 1] The information record medium characterized by to record the condition information at the time of decrypting the above-mentioned encryption information in the information record medium with which the encryption information enciphered, the encryption key information which enciphered the key information for decrypting this encryption information to the information on original, and \*\* are recorded after having been un-enciphered by the above-mentioned encryption key information.

[Claim 2] The information record medium according to claim 1 characterized by the above-mentioned condition information being the conditions which show authorization of encryption of the above-mentioned encryption information.

[Claim 3] The information record medium according to claim 2 characterized by being that in which the above-mentioned condition information includes the device information which shows the device using the information which had the transmission route of the above-mentioned encryption information, and the above-mentioned encryption information enciphered.

[Claim 4] The information record medium according to claim 2 characterized by the above-mentioned condition information being a thing including field information.

[Claim 5] The information record medium according to claim 2 characterized by the above-mentioned condition information being a thing including time information.

[Claim 6] The information record medium according to claim 2 characterized by being that in which the above-mentioned condition information includes the information which limits a user.

[Claim 7] The information record medium according to claim 1 characterized by the above-mentioned condition information being the device information which shows the device using the information which had the transmission route of the above-mentioned encryption information, and the above-mentioned encryption information enciphered.

[Claim 8] The information record medium according to claim 7 characterized by the above-mentioned condition information being a thing including field information.

[Claim 9] The information record medium according to claim 7 characterized by the above-mentioned condition information being a thing including time information.

[Claim 10] The information record medium according to claim 7 characterized by being that in which the above-mentioned condition information includes the information which limits a user.

[Claim 11] The information record medium according to claim 1 with which the above-mentioned condition information is characterized by being field information.

[Claim 12] The information record medium according to claim 11 characterized by the above-mentioned condition information being a thing including time information.

[Claim 13] The information record medium according to claim 11 characterized by being that in which the above-mentioned condition information includes the information which limits a user.

[Claim 14] The information record medium according to claim 1 with which the above-mentioned condition information is characterized by being time information.

[Claim 15] The information record medium according to claim 14 characterized by being that in which the above-mentioned condition information includes the information which limits a user.

[Claim 16] The information record medium according to claim 1 characterized by the above-mentioned condition information being the information which limits a user.

[Claim 17] A setting-out means to set up the condition information at the time of decrypting with encryption key draft proposal information, The 1st generation means which generates encryption key information using the condition information in the condition of having been un-enciphered as the encryption key draft proposal information set up by this setting-out means, The 2nd generation means which decrypts the encryption key information generated by record means to record common key information, and the generation means of the above 1st using the common key information currently recorded on the above-mentioned record means, and generates key information, The 3rd generation means which enciphers the information which was inputted by input means to input the information to encipher, and this input means, and to encipher using the key information generated by the generation means of the above 2nd, and generates encryption information, The recording device characterized by providing a record means to record on an information record medium after encryption key information including the condition information generated by the generation means of the above 1st and the encryption information generated by the generation means of the above 3rd have corresponded.

[Claim 18] The recording device according to claim 17 characterized by the above-mentioned condition information being the conditions which show authorization of encryption of the above-mentioned encryption information.

[Claim 19] The recording device according to claim 17 characterized by the above-mentioned condition information being the device information conditions which show the device using the information which had the transmission route of the above-mentioned encryption information, and the above-mentioned encryption information enciphered.

[Claim 20] The recording device according to claim 17 with which the above-mentioned condition information is characterized by being field information.

[Claim 21] The recording device according to claim 17 with which the above-mentioned condition information is characterized by being time information.

[Claim 22] The recording device according to claim 17 characterized by the

above-mentioned condition information being the information which limits a user.

[Claim 23] The 1st equipment which has the information record medium with which the encryption information enciphered and the encryption key information which enciphered the key information for decrypting this encryption information to the information on original are recorded, In the information transmission system which consists of the 2nd equipment with which it connects with this 1st equipment through a communication line, and the encryption information and encryption key information from an information record medium on the 1st equipment of the above are transmitted The condition information at the time of decrypting the above-mentioned encryption information in the condition of having been un-enciphered is recorded on the encryption key information recorded on the information record medium of the 1st equipment of the above. The 1st equipment of the above consists of a transmitting means to transmit encryption key information including the condition information currently recorded on the above-mentioned information record medium, and encryption information to the 2nd equipment of the above. The 1st output means outputted to the processing medium by which the 2nd equipment of the above processes a decryption of the condition information, encryption key information, and encryption information from the 1st equipment of the above, A decision means to judge whether it consists of an activation means to perform processing according to the information decrypted from the above-mentioned processing medium, and the above-mentioned processing medium permits a decryption based on the condition information from the 2nd equipment of the above, A decryption means to decrypt encryption information based on the encryption key information from the 2nd equipment of the above when authorization of a decryption is judged with this decision means, The information transmission system characterized by what is consisted of the 2nd output means which outputs the information decrypted by this decryption means to the 2nd equipment of the above.

[Claim 24] In the thing treating the encryption information enciphered and the encryption key information which enciphered the key information for decrypting

this encryption information to the information on original A record means by which the 2nd specific information generated by the 1st specific information and common key information is recorded, A generation means to generate the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, The 1st decryption means which decrypts the above-mentioned encryption key information using the common key information generated by the above-mentioned generation means, and acquires key information, Decryption equipment characterized by providing the 2nd decryption means which decrypts the above-mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption.

[Claim 25] In the portable medium treating the encryption information enciphered and the encryption key information which enciphered the key information for decrypting this encryption information to the information on original The 1st generation means which generates the 2nd specific information using the input section into which the 1st specific information and common key information are inputted, and the 1st specific information inputted from this input section and common key information, A record means to record the 2nd specific information generated by this 1st generation means, A prohibition means to forbid the input from the above-mentioned input section after recording on this record means, The 2nd generation means which generates the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, The 1st decryption means which decrypts the above-mentioned encryption key information using the common key information generated by the generation means of the above 2nd, and acquires key information, Decryption equipment characterized by providing the 2nd decryption means which decrypts the above-

mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption.

[Claim 26] In the thing treating the encryption key information which enciphered the key information for decrypting the above-mentioned encryption information to the information on original including the encryption information enciphered and the condition information at the time of decrypting this encryption information A record means by which the 2nd specific information generated by the 1st specific information and common key information is recorded, A generation means to generate the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, The 1st decryption means which decrypts the above-mentioned encryption key information using the common key information generated by the above-mentioned generation means, and acquires key information, The 2nd decryption means which decrypts the above-mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption, Decryption equipment characterized by providing a decision means to judge whether a decryption is permitted using the above-mentioned condition information, and the control means which controls activation of the decryption by the above 1st and the 2nd decryption means by this decision means based on a decision result.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the information record medium with which the encryption information enciphered and the encryption key information which enciphered the key information for decrypting this encryption information to the information on original are recorded, the recording device of this information record medium, the information transmission system which transmits the information from an information record medium to other devices, and decrypt it, and the decryption equipment which decode encryption information to the information on original using encryption key information.

[0002]

[Description of the Prior Art] The information acquisition in the world is possible using current and the Internet. Recently, the close accounting system to the data utility in a specific domain (a field, area) is also in a fractional replication phase. Security reservation aiming at unjust prevention also serves as pressing need with the Internet spread.

[0003] It may prevent the case (prevention of information usurpation) where it is prevented that specify the user who receives A service as an object of the security which should be secured, enter as the 3rd person is a signal transduction path, and service information seizes, and that infringe on B copyright and the 3rd person other than a service provider uses the service information on original for other commercial objects (prevention of an information duplicate).

[0004] It is expected that the request about the information duplicate prevention especially raised to (B) will be increased by quickly from now on. This is because development of current and a network computer is furthered energetically.

[0005] The network computer under current development does not build in HDD, but calls even OS from a host server on radio at the time of a startup, and is an object which works application software required for an activity while installing a required functional program on radio when required.

[0006] Therefore, conventionally, a user purchases various application software packages and uses, installing in HDD. However, when a network computer is



used, prior purchase becomes unnecessary, and it serves as a system charged whenever it calls a functional program while it calls and uses a required functional program, when required. This functional program is a very small-scale program which there is not and was described by JAVA etc. in a large-scale program like a package program and by which functional definition was carried out.

[0007] Therefore, when a network computer is used, there is the need of forbidding the duplicate and reuse of the functional program by the user, from the particulars of the accounting approach. as the approach of the above-mentioned security reservation -- ASHIN -- metric (object cryptosystem) one -- there are the following three approaches using encoding technology.

1. A public key and a private key are published by the user side, and a public key is communicated with a data utility claim to an information service provider.
2. An information service provider enciphers service information with a radical to the public key which I had sent from a user, and sends to a user.
3. Encryption information is decrypted and used using the private key which he published by the user side.

[0008] However, when these approaches are used, whenever there is a demand from a user, it will be necessary to encipher, and, as for an information service provider, service cost will start substantially.

[0009] As an approach of avoiding it, the symmetric (cryptosystem for un-) method using a common key common, at the time of encryption and a decryption is adopted, and there is also the approach of adopting the system by which only the user who knows delivery and a common key can decode the common key enciphered to the enciphered service information and coincidence to a user.

[0010] However, when this approach is used, the following problems arise.

a] It will be reproduced by the user at HDD or an optical disk, and service information cannot be charged for every data utility like a network computer at him.

As long as a b] common key is made in agreement, it becomes easy to divert

unjustly information [ that the 3rd person other than an information service provider is enciphered ] to commerce.

[0011] Although data utility using a computer network has mainly been explained in the above explanation, the service using satellite broadcasting service exists similarly. When broadcast is used, an ASHIN metric method (approach using a public key and a private key) cannot be used, but adopts the symmetric method using a public key, and only the specific user who knows the public key can make it possible to receive service.

[0012] However, the problem of the above-mentioned [a] and [b] occurs in common also in this case. Moreover, the above trouble is specified from a viewpoint of encoding technology. By the common key (symmetric) method for which a reception place uses the same key, there are the following three faults a sending agency as known conventionally.

1) The danger by the 3rd person of being copied illegally is during a transfer of a key.

2) Management of a key is complicated.

3) The alteration of the code data itself can be easily performed at a reception place. That is, at a reception place, with a common key, after a decryption, after altering code data, it is made as for enciphering with a common key again to preparation.

[0013] On the other hand, although the above-mentioned trouble improves by the ASHIN metric method using a public key and a private key, there are the following faults.

\*\*] Processing of encryption/decryption takes huge time amount.

\*\*] Whenever an information service provider sends information to a user, it is necessary to ask CA center (certificate authority) the public key for every user.

[0014] The burden by the side of the information service provider to say increases. Furthermore, a great burden is hung on a user about storage of the Ha] private key.

[0015] For example, security reservation becomes impossible only by a private

key being stolen. Moreover, since close [ of a private key ] can reproduce easily FD and the IC card which are by the user side, there is a danger that the reproduced private key information will be abused.

[0016] There is also a problem to say. The hybrid system of enciphering the data itself with a common key and enciphering only this common key again with a public key as an approach of improving the above-mentioned problem is proposed. If this method is used, although "hypertrophy of the processing time of [I] encryption / decryption" is eased, the complicatedness of [RO] and [Ha] will not be mitigated.

[0017] Moreover, in also transmitting or recording the key used for informational encryption, in order to keep a key secret, it transmits or records transmitting or recording the key which used for encryption as it is in the system which enciphers information, and transmits or records as key information which enciphered the key separately with the encryption means other than an informational encryption means, without carrying out. In an information playback side, encryption information is decrypted with an informational decryption means using the key which decrypted key information with the decryption means of a key first, and was obtained.

[0018] As this is used and playback control information is included in the key before encryption, how to prevent the alteration of playback control information can be considered. However, in order to know playback control information to an information playback side in case of this approach, key information must be decrypted, and it becomes a big problem when that is the following information regeneration systems.

[0019] For example, the decryption means of encryption information does not have the decryption means of key information, either, but the disk drive equipment which reads the only recorded data is made to judge playback prohibition information, and the information regeneration system it was made to make the data transfer to an information regenerative apparatus with a decryption means control is explained.

[0020] In this case, it is because the serious problem that also having to give the decryption means of key information to disk drive equipment, and causing the increment in cost of disk drive equipment causes lowering of the security of the whole system by, of course giving a decryption means to decrypt unnecessary key information to disk drive equipment is caused.

[0021]

[Problem(s) to be Solved by the Invention] Since the encryption processing for every user demand of a host server becomes unnecessary, the information delivery of the object of this invention is attained by low cost. The object of this invention can discover an informational illegal copy very easily, and can raise security substantially.

[0022] The object of this invention has few dangers of being copied illegally according, to the 3rd person under transfer of a key to the fault of a common key system, management of a key is easy for it, and the point said that the alteration of the code data in a reception place is difficult is improved substantially.

[0023] The point which shows the object of this invention below compared with an ASHIN metric method is improved substantially. Encryption/decryption processing is relatively easy for provider side / user side of data utility, and it can be processed in a short time.

[0024] That an information service provider side should set up only a master key, since it is not necessary to ask the public key to the management center for every user, the information offer activity to a user can increase the efficiency substantially.

[0025] The information service provider side records the information enciphered in advance on the IC card side, and can deliver it as it is. For this reason, compared with the conventional cipher system which enciphers and carries out information delivery for every demand of a user, the burden by the side of an information service provider improves substantially.

[0026] Preparation of a decryption is completed only in the conventional authentication procedure of entering a user password into the personal

authentication using an IC card. Therefore, encoding technology can be adopted, without newly forcing a burden upon a user for security reservation.

[0027] Since device information and field information are included in the control information of encryption key information, the information enciphered by the user side is copied to HDD or an optical disk as it is, and it can prevent using improperly. Consequently, all the faults of the conventional encoding technology are improved, and information sending origin and a reception place can simplify processing substantially, and can strengthen a security function.

[0028]

[Means for Solving the Problem] the encryption information enciphered and the encryption key information which enciphered the key information for decrypting this encryption information to the information on original are recorded, the information record medium of this invention is set, and the condition information at the time of decrypting the above-mentioned encryption information, after having been un-enciphered by the above-mentioned encryption key information is recorded.

[0029] A setting-out means to set up the condition information at the time of decrypting the recording device of this invention with encryption key draft proposal information, The 1st generation means which generates encryption key information using the condition information in the condition of having been un-enciphered as the encryption key draft proposal information set up by this setting-out means, The 2nd generation means which decrypts the encryption key information generated by record means to record common key information, and the generation means of the above 1st using the common key information currently recorded on the above-mentioned record means, and generates key information, The 3rd generation means which enciphers the information which was inputted by input means to input the information to encipher, and this input means, and to encipher using the key information generated by the generation means of the above 2nd, and generates encryption information, It consists of a record means to record on an information record medium after encryption key

information including the condition information generated by the generation means of the above 1st and the encryption information generated by the generation means of the above 3rd have corresponded.

[0030] The 1st equipment which has the information record medium with which the encryption key information which enciphered key information for the information transmission system of this invention to decrypt the encryption information enciphered and this encryption information to the information on original is recorded, In what consists of the 2nd equipment with which it connects with this 1st equipment through a communication line, and the encryption information and encryption key information from an information record medium on the 1st equipment of the above are transmitted The condition information at the time of decrypting the above-mentioned encryption information in the condition of having been un-enciphered is recorded on the encryption key information recorded on the information record medium of the 1st equipment of the above. The 1st equipment of the above consists of a transmitting means to transmit encryption key information including the condition information currently recorded on the above-mentioned information record medium, and encryption information to the 2nd equipment of the above. The 1st output means outputted to the processing medium by which the 2nd equipment of the above processes a decryption of the condition information, encryption key information, and encryption information from the 1st equipment of the above, A decision means to judge whether it consists of an activation means to perform processing according to the information decrypted from the above-mentioned processing medium, and the above-mentioned processing medium permits a decryption based on the condition information from the 2nd equipment of the above, When authorization of a decryption is judged with this decision means, it consists of a decryption means to decrypt encryption information based on the encryption key information from the 2nd equipment of the above, and the 2nd output means which outputs the information decrypted by this decryption means to the 2nd equipment of the above.

[0031] In the thing treating the encryption key information which enciphered key information for the decryption equipment of this invention to decrypt the encryption information enciphered and this encryption information to the information on original A record means by which the 2nd specific information generated by the 1st specific information and common key information is recorded, A generation means to generate the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, It consists of the 1st decryption means which decrypts the above-mentioned encryption key information using the common key information generated by the above-mentioned generation means, and acquires key information, and the 2nd decryption means which decrypts the above-mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption.

[0032] In the portable medium treating the encryption key information which enciphered key information for the decryption equipment of this invention to decrypt the encryption information enciphered and this encryption information to the information on original The 1st generation means which generates the 2nd specific information using the input section into which the 1st specific information and common key information are inputted, and the 1st specific information inputted from this input section and common key information, A record means to record the 2nd specific information generated by this 1st generation means, A prohibition means to forbid the input from the above-mentioned input section after recording on this record means, The 2nd generation means which generates the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, It consists of the 1st decryption means which decrypts the above-mentioned encryption key information using the common key



information generated by the generation means of the above 2nd, and acquires key information, and the 2nd decryption means which decrypts the above-mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption.

[0033] In the thing treating the encryption key information which enciphered the encryption information as which the decryption equipment of this invention is enciphered, and the key information for decrypting the above-mentioned encryption information to the information on original including the condition information at the time of decrypting this encryption information A record means by which the 2nd specific information generated by the 1st specific information and common key information is recorded, A generation means to generate the above-mentioned common key information by setting-out means to set up the 1st specific information, and the 1st specific information set up by this setting-out means and the 2nd specific information currently recorded on the above-mentioned record means, The 1st decryption means which decrypts the above-mentioned encryption key information using the common key information generated by the above-mentioned generation means, and acquires key information, The 2nd decryption means which decrypts the above-mentioned encryption information using the key information acquired by the decryption means of the above 1st, and acquires the information before encryption, It consists of a decision means to judge whether a decryption is permitted using the above-mentioned condition information, and a control means which controls activation of the decryption by the above 1st and the 2nd decryption means by this decision means based on a decision result.

[0034]

[Embodiment of the Invention] Hereafter, the optical disk regenerative apparatus applied to the example of this invention with reference to a drawing is explained. Hereafter, the gestalt of implementation of the 1st of this invention is explained with reference to a drawing.

[0035] Drawing 1 shows the information transmission system of this invention. This information transmission system is constituted by IC card 4 as the host server 3 connected with a client machine 1 and this client machine 1 through a communication line 2, and the decryption section loaded with or built in a client machine 1.

[0036] That is, the transfer request of programs, such as word-processing software, is transmitted to the host server 3 as predetermined data of a client machine 1. According to this transmission, programs (encryption information), such as word-processing software which is recorded on the hard disk drive unit (HDD) 29 as the Records Department which the host server 3 mentions later according to that transfer request and which is enciphered, are returned to the client machine 1 which had the transfer request with the encryption key information (enciphered for the information for decrypting) corresponding to that encryption information. According to this return, a client machine 1 decrypts encryption information using encryption key information using IC card 4 (decode), and can be processed now using programs, such as this decrypted word-processing software.

[0037] It is recorded on the above-mentioned hard disk drive unit (HDD) 29 for every service information with which a user is provided. As this service information, the functional program of the subunit for applications described for example, not only in mere specific data but in programming (java) language etc. is included.

[0038] The example of structure of one service information currently recorded on the above-mentioned hard disk drive unit (HDD) 29 is explained using drawing 2. That is, the information which consists of encryption key information 41 that the key information which decrypts a program (information which a user uses) 40 and these encryption information 40, such as word-processing software enciphered as encryption information, (decode) is enciphered is recorded.

[0039] In the encryption key information 41, control information 42 is included in the form un-enciphered by the part (in form which can be read directly). Control

information 42 is the condition information at the time of decrypting corresponding encryption information 40 (decode).

[0040] Control information 42 serves as 119 bit patterns which consist of a specific user / organization information 50 on 49 or 32 bits of specific password information of 48 or 24 bits of copy prohibition period information after the information creation of 47 or 7 bits of information creation date information of the address code 45 of 44 or 32 bits of drive codes of 43 or 4 bits of 1 bit of copy authorization codes, and 46 or 16 bits of region codes of a triplet, as shown in drawing 3 .

[0041] The drive code 44 and the address code 45 are calling it the device information 51. The region code 46 is calling it field information. The information creation date information 47 and the copy prohibition period information 48 are called the time information 52. The specific password information 49, and the specific user / organization information 50 are called the user limited information 53.

[0042] Authorization of a copy and disapproval are shown, copy authorization is shown at the time of "1", and the copy authorization code 43 shows copy disapproval at the time of "0." The drive code 44 shows the information-transmission path and the activity drive.

[0043] The information-transmission path shows the ISDN(LAN network)10MHz response at the time of "1H (hexa: hex decimal)." The signal transduction path shows the ISDN(LAN network)100MHz response at the time of "2 H".

[0044] The signal transduction path shows the ISDN(LAN network)500MHz response at the time of "3 H". The signal transduction path shows the general wire telephone line (modem utilization) at the time of "4 H".

[0045] The signal transduction path shows the ground wave (multiplex TV channel) at the time of "5 H". The signal transduction path shows satellite broadcasting service at the time of "6 H". The signal transduction path shows radiocommunication (PHS, cellular telephony network) at the time of "7 H".

[0046] The signal transduction path shows partial radiocommunication (a

domestic communication link, business communication link within a station) at the time of "8 H". When signal transduction paths are a cable network and "AH" at the time of "9 H", the signal transduction path (activity drive) shows FDD.

[0047] The signal transduction path (activity drive) shows Boot (the operation system at the time of starting is recorded) HDD at the time of "CH." The signal transduction path (activity drive) shows optical disks, such as MO and PD, at the time of "DH."

[0048] The signal transduction path (activity drive) shows CD-ROM and CD-R at the time of "EH." The signal transduction path (activity drive) shows DVDVideo and DVD-ROM at the time of "FH."

[0049] As for DVD-RAM \*\*\*\*, the signal transduction path (activity drive) shows DVD-R at the time of "0 H". An address code 45 shows the address data (IP address) for identifying transmission place and transmitting origin, for example, consists of a network address and the host address. This address code 45 is given when signal transduction is ISDN (LAN network).

[0050] A region code 46 divides the area on the earth into eight areas, and gives the number of 1H to 8H with hex decimal for every every place region. The region code 46 supports field information.

[0051] The information creation date information 47 shows the information creation date, and is described by 7 bits year information, 4 bits moon information, and 5-bit Japanese information. The copy prohibition period information 48 shows a copy prohibition period, i.e., copy disapproval length, and when a copy authorization code is the copy disapproval of "0", it is given. This copy prohibition period information 48 can be described till a maximum of ten-year and seven month = 127 months, and, in the case of "0000000", shows the prohibition on a copy eternally.

[0052] The specific password information 49 shows the specific password shown by four characters of the alphabet and a figure, and can choose now 36 kinds of alphabetic characters as every one character. In this case, one character is described at a time by the code which is 6 bits.

[0053] A specific user / organization information 50 shows a specific user and an organization. You may make it simplify the content of the above-mentioned control information 42 according to the content of information (contents) dealt with with an information transmission system. For example, as a simple system, control information 42 may consist of only copy authorization codes 43 which are 1 bit.

[0054] The control information 42 which has the structure shown in above-mentioned drawing 3 is inserted in in the encryption key information 41 shown in drawing 2 as it is. The size of this encryption key information 41 is larger than the size of control information 42, in order to prevent decode of the encryption key information 41 by the hacker, also at the lowest, the size of the encryption key information 41 is required, and the twice of control information 42 have 3 or more times actually desirable [ size ].

[0055] Therefore, when the above-mentioned control information 42 is 119 bit patterns, as for the encryption key information 41, the minimum or 238 bits, and 357 bits or more also of usual are also needed. Moreover, when control information 42 consists of only 1-bit copy authorization codes 43, as for the encryption key information 41, the minimum or 2 bits, and usual are needed more than a triplet.

[0056] IC card 4 has the polar zone 5 as the connection section connected to IC card reader writer 13 mentioned later, the hole 6 for user password input terminals, and the hole 7 for master key input terminals, as shown in drawing 4 . User password input terminal 6a is in the hole 6 for user password input terminals, and master key input terminal 7a is in the hole 7 for master key input terminals.

[0057] In case the hole 6 for user password input terminals and the hole 7 for master key input terminals are published by the issuance equipment of IC card 4, the key information (the 2nd specific information) corresponding to a user is generated by the input of a user password (the 1st specific information) and master key information (common key information), and after being recorded on

EEPROM34 mentioned later, they are embedded by resin enclosure etc.

Thereby, the key information corresponding to a user cannot be changed afterwards, that is, it can be made not to carry out the unjust alteration.

[0058] That is, by the input of the user password as the 2nd specific information entered by the user, i.e., the provider who is the publisher of IC card 4, and a master key, after forming the key information corresponding to a user as the 1st specific information, the input path from the outside to the input section (input terminal) is intercepted for alteration prevention.

[0059] Moreover, you may prevent from changing key information corresponding to a user afterwards by removing user password input terminal 6a and the master key input terminal 7a itself, or removing those electrode sections instead of the hole 6 for user password input terminals and the hole 7 for master key input terminals being filled. In this case, you may make it remove by using lead wire instead of an input terminal, and drawing out lead wire at the time of issuance.

[0060] As client machines 1 are information management systems, such as a personal computer, and are shown in drawing 5 As CPU10 which controls the whole client machine 1, ROM11 on which the control program is recorded, RAM12 for data logging, IC card reader writer 13 which exchanges data between above-mentioned IC cards 4, a display 14, and the input section As the Records Department by which it is loaded with the \*\* keyboard 15, the hard disk drive unit (HDD) 16 as the Records Department (information record medium), and optical disk 17a It is constituted by \*\*\*\*\* 17 and the communication link interface 18 connected with the host server 3 through the above-mentioned communication line 2.

[0061] A hard disk drive unit (HDD) 16 and an optical disk unit 17 are later connectable with an option. As shown in drawing 6 , the host server 3 CPU20 which controls the whole host server 3, ROM21 on which the control program is recorded, RAM22 for data logging, EEPROM23 on which master key information is recorded beforehand, and raw information using key information The code machine 24 and the encryption key information 41 that encryption to the

encryption information 40 is performed using master key information As the decoder 25 which performs the decryption to key information, the key information-synthesis machine 26 which generates the encryption key information 41, and a display As the input section into which a user enters \*\* CRT display 27 and a user password As the Records Department (information record medium) where the information which consists of programs (encryption information), such as the \*\* keyboard 28 and word-processing software enciphered, and encryption key information corresponding to this encryption information is recorded It is constituted by the communication link interface 30 connected with a client machine 1 through the \*\* hard disk drive unit (HDD) 29 and the above-mentioned communication line 2.

[0062] An optical disk unit may be used instead of the above-mentioned hard disk drive unit (HDD) 29. Furthermore, when considering as the mass Records Department, you may make it constituted by disk arrays, such as RAID (redundant arrays inexpensive disk).

[0063] The above-mentioned key information-synthesis machine 26 performs composition with the encryption key draft proposal information as an encryption key, and control information 42 provisionally, generates the encryption key information 41 as a synthetic result, and as shown in drawing 7 , it is constituted by two shift registers 26a and 26b.

[0064] Thereby, when the sequential output of the encryption key draft proposal information supplied is carried out and the load signal from CPU20 is supplied, by loading control information 41, shift registers 26a and 26b insert control information 41 in the encryption key draft proposal information, and output it to it. Under the present circumstances, a load signal is outputted based on the address of the encryption key draft proposal information which reads CPU20 from RAM22.

[0065] The above-mentioned code machine 24 and the decoder 25 are constituted by seven shift registers 60a-60g and the computing elements 61a-61c which perform three EXCLUSIVE OR operation as shown in drawing 8 ,

respectively.

[0066] In the case of the code machine 24, when the key information "1010010001011" as a random number is supplied to shift registers 60a-60g and raw information "1110001110001" is supplied to computing-element 61c, encryption information "1011100000101" is outputted from computing-element 61c as an encryption result.

[0067] In the case of a decoder 25, when the master key information "110100000110" as a random number is supplied to shift registers 60a-60g and encryption key information "1000011100101" is supplied to computing-element 61c, the key information "1010010001011" as decryption information is outputted from computing-element 61c as a decryption result.

[0068] In addition, although the keyboard 28 is used as the input section which enters a user password, a voiceprint is used instead of a user password and you may make it use a microphone and a voiceprint feature detection machine as the input section. Moreover, you may make it use the face image read station and face information feature-extraction machine which use face information instead of and consist of CCD etc. as the input section. [ a user password ] Moreover, the speech recognition of a password is used instead of the key input of a user password, and you may make it use a microphone and a voice recognition unit as the input section. Moreover, you may make it use the fingerprint read station and image feature-extraction machine which use a fingerprint instead of and consist of CCD etc. as the input section. [ a user password ] Moreover, you may make it use the finger surface-electrical-resistance value measuring device in each point and finger information feature-extraction equipment to use finger information instead of and according to an electrode array as the input section. [ a user password ]

[0069] CPU31 as for which above-mentioned IC card 4 controls whole IC card 4 to be shown in drawing 9 , ROM32 on which the control program is recorded, RAM33 for data logging, the key information corresponding to a user, A user password, The key information generation machine 35 corresponding to the user



who generates EEPROM34 and the key information corresponding to a user on which user ID etc. is recorded, the master key generation machine 36 which generates master key information, and the encryption key information 41 using master key information User password input terminal 6a into which the decoder 38 which performs the decryption to raw information using key information, an interface 39, the connection section 5, and a user password are entered in the decoder 37 which performs the decryption to key information, and the encryption information 40, It is constituted by master key input terminal 7a into which master key information is inputted.

[0070] Above-mentioned IC card 4 is giving the user individual IC card 20 for authentication for reservation of security, and all decryption circuits are built in in this IC card 20. By this method, neither the master key information 6 nor the key information 3 came out of IC, and the injustice by the hacker is prevented.

Therefore, in the information transmission system shown in drawing 1 , IC card 20 with which the decryption circuit is built in is decryption equipment, and when it sees from the whole information transmission system, it is equivalent to the decryption section.

[0071] The key information generation machine 35 corresponding to a user consists of computing elements which perform EXCLUSIVE OR operation, and generates the key information corresponding to a user as the result of an operation by performing EXCLUSIVE OR operation of the master key information that it is inputted from the user password entered from user password input terminal 6a, and master key input terminal 7a.

[0072] For example, the operation of a user password "1100" and master key information "1010" generates the key information "1001" corresponding to a user. The master key generation machine 36 consists of computing elements which perform EXCLUSIVE OR operation, and generates master key information as the result of an operation by performing EXCLUSIVE OR operation of the user password supplied from the key information corresponding to a user read from EEPROM34, and the outside.

[0073] For example, the operation of the key information "1001" corresponding to a user and a user password "1100" generates master key information "1010."

The above-mentioned decoders 37 and 38 are constituted by the random number generator which consists of seven shift registers 60a-60g and computing elements 61a-61c which perform three EXCLUSIVE OR operation as shown in drawing 8 , respectively. This calculates using the information serially supplied to computing-element 61c to the information loaded to shift registers 60a-60g.

[0074] In the case of a decoder 37, when the master key information "110100000110" as a random number is supplied to shift registers 60a-60g and encryption key information "1000011100101" is supplied to computing-element 61c, the key information "1010010001011" as decryption information is outputted from computing-element 61c as a decryption result.

[0075] In the case of a decoder 38, when the key information "1010010001011" as a random number is supplied to shift registers 60a-60g and encryption information "1011100000101" is supplied to computing-element 61c, the raw information "1110001110001" as decryption information is outputted from computing-element 61c as a decryption result.

[0076] Next, it explains, referring to drawing showing the generation process of the flow chart shown in drawing 10 , the encryption key information 41 on drawing 11 , and the encryption information 40 about the record approach of the service (it provides for user) information on the hard disk drive unit (HDD) 29 by the host server 3 mentioned above.

[0077] For example, the provider (the service information to a user is offered) of the host server 3 inputs now the raw information as a functional program of the subunit for applications described in programming (java) language etc., using the user interface which consists of CRT display 27 and a keyboard 28 (ST1). This raw information is recorded on RAM22 by CPU20 (ST2).

[0078] Furthermore, the provider of the host server 3 inputs the content of the control information 42 which consists of code authorization code 43 grade as shown in drawing 7 mentioned above using a user interface (ST3). This control

information 42 is recorded on RAM22 by CPU20 (ST4).

[0079] Furthermore, the provider of the host server 3 inputs the encryption draft proposal information as an encryption key provisionally using a user interface (ST5). This encryption draft proposal information is recorded on RAM22 by CPU20 (ST6).

[0080] And by outputting the encryption draft proposal information and control information 42 which are recorded on RAM22 to read-out and the key information-synthesis machine 26, CPU20 makes the key information-synthesis machine 26 perform synthetic processing with encryption draft proposal information and control information 42, and generates the encryption key information 41 (ST7). Subsequently, CPU20 is recorded on a hard disk drive unit (HDD) 29 while it records this generated encryption key information 41 on RAM22 (ST8).

[0081] Subsequently, by outputting the encryption key information 41 which is recorded on RAM22 and by which generation was carried out [ above-mentioned ], and the master key information currently recorded on EEPROM23 to read-out and a decoder 25, CPU20 makes a decoder 25 perform processing which decrypts encryption key information 41 using master key information (decode), and generates key information (ST9). Subsequently, CPU20 records this generated key information on RAM22 (ST10).

[0082] Subsequently, by outputting the key information by which generation was carried out [ above-mentioned ] with the raw information currently recorded on RAM22 to read-out and the code machine 24, CPU20 makes the code machine 24 perform processing which enciphers raw information using key information, and generates the encryption information 40 (ST11). Subsequently, this generated encryption information 40 is made equivalent to the above-mentioned encryption key information 41, and CPU20 records it on a hard disk drive unit (HDD) 29 (ST12).

[0083] In this case, the encryption key information 41 is made previously first, key information is generated for the first time through that after decoder, the

encryption information 40 which is the service information supplied to a user with a code vessel using this generated key information is generated, and this generated encryption information 40 is recorded on HDD29 with the above-mentioned encryption key information 40.

[0084] Next, it explains, referring to the flow chart shown in drawing 12 about the registration approach into the issuance processing 4 of above-mentioned IC card 4 by the information service provider, i.e., the IC card of the key information corresponding to a user. Before IC card 4 arrives to a user fundamentally, an information service provider sets up.

[0085] The issuance machine which publishes this IC card 4 consists of a card reader writer which can input through user password input terminal 6a and master key input terminal 7a, a user interface which consists of a display and the input section, and a control section which controls issuance processing while being able to perform an exchange of the connection section 5 of above-mentioned IC card 4, and data.

[0086] That is, an information service provider inserts in the above-mentioned issuance machine IC card 4 with which no records are made (ST21). Thereby, the card reader writer of an issuance machine, and the connection section 5 of IC card 4, user password input terminal 6a and master key input terminal 7a are connected (ST22).

[0087] Furthermore, an information service provider inputs the user password which the information service provider determined at the time of an agreement with a user, and the master key information which only the information service provider knows while directing issuance of an IC card by the user interface (ST23). Thereby, a user password and master key information are supplied to the key information generation machine 35 corresponding to a user through IC card reader writer 13 and user password input terminal 6a, and master key input terminal 7a (ST24). Then, by performing EXCLUSIVE OR operation of the bitwise of those information, the key information generation machine 35 corresponding to a user generates the key information corresponding to a user,

and outputs it to EEPROM34 (ST25). Thereby, the key information corresponding to a user is recorded on EEPROM34 (ST26).

[0088] Moreover, after the key information corresponding to a user is recorded, an information service provider inputs the user password and user ID which were decided at the time of an agreement with a user. Thereby, CPU10 outputs a user password and user ID to CPU31 through IC card reader writer 13, the connection section 5, and an interface 39. CPU31 records the user password and user ID which are supplied on EEPROM34.

[0089] After the above-mentioned key information corresponding to a user etc. is recorded, IC card 4 is published from the above-mentioned issuance machine. The hole 6 for user password input terminals and the hole 7 for master key input terminals are embedded by the provider by resin enclosure etc. to this published IC card 4. Thereby, the input path from the outside to the key information generation machine 35 corresponding to a user can be intercepted, the key information corresponding to a user cannot be changed afterwards, that is, an unjust alteration can be prevented.

[0090] Next, the starting processing in a client machine 1 performs the transfer request of programs, such as word-processing software, to the host server 3, the information which is acquired according to this demand and which is enciphered is decoded with IC card 4, and it explains, referring to the flow chart shown in drawing 13 about the processing set up as a functional program.

[0091] First, the power source which a client machine 1 does not illustrate is turned on, and a client machine 1 is started (ST31). Then, a client machine 1 checks whether specific groups (accounting system etc.) have data needed by the exchange with the host server 3 (ST32). For example, programs, such as word-processing software as data utility, are requested. When this check (request) is directed, CPU10 guides insertion of IC card (it is decipherable) 4 which can call the above-mentioned data by the display 14 (ST33). According to this advice, a user inserts corresponding IC card 4 (ST34).

[0092] Subsequently, CPU10 guides the input of user ID and a user password by

the display 14 (ST35). According to this advice, a user enters user ID and a user password (ST36).

[0093] This user ID and user password that were entered are supplied to CPU31 in IC card 4 by CPU10 through IC card reader writer 13, the connection section 5, and an interface 39 (ST37). The user ID and the user password with which CPU31 was supplied by this, and the user ID currently recorded on EEPROM23 in advance are compared with a user password, respectively, it judges whether it is in agreement (ST38), and at the time of coincidence, user ID is notified to a client machine 1 (ST39), it is regarded as injustice at the time of an inequality, actuation is suspended, and NG signal is notified to a client machine 1 (ST40).

[0094] At the time of coincidence of the decision result by the above-mentioned step 38, in parallel to processing of step 39, CPU31 performs EXCLUSIVE OR operation for the above-mentioned user password and the key information corresponding to a user currently recorded on EEPROM34 in advance with the master key generation vessel 36, generates master key information as the result of an operation, and records it on RAM33 (ST41).

[0095] The client machine 1 with which user ID was notified by the above-mentioned step 39 gives the IP address of a client machine 1 to the information service request based on the request of programs, such as word-processing software as data utility by the user who mentioned above, and the user ID obtained from IC card 4, and transmits it to the host server 3 (ST42). This host server 3 accepts that transfer request. After attesting user ID, As data utility which is enciphered by the hard disk drive unit (HDD) 29, and is recorded on it The address of a transmission place puts close into the communication link packet which gave the IP address to require transmitting-to programs [ , such as \*\* word-processing software, ] (encryption information 40) and encryption key information 41 (enciphered for information for decrypting) corresponding to the encryption information origin. The client machine 1 with a transfer request is returned (ST43). Under the present circumstances, it is recorded on the Records Department which the content of accounting to the user of the above-mentioned

user ID does not illustrate as transmission of data utility.

[0096] According to the above-mentioned return, a client machine 1 decrypts encryption information 40 using IC card 4 by the control information 42 within the encryption key information 41 and this encryption key information 41 (decode) (ST44), and can be processed now using programs, such as this decrypted word-processing software, (ST45).

[0097] It explains referring to the flow chart shown in drawing 14 about decryption processing of the above-mentioned encryption information 40. Namely, CPU10 of a client machine 1 consists of a region code which judged the region code of the area in which the host server 3 is installed by the IP address in the communication link packet which received, and was judged to be the IP address of the transmitting origin, when it is the LAN network whose communication line 2 is 10MHz, as mentioned above, it creates the client machine creation information which added "1H" which is the value of the drive code 44, and it sends it to IC card 4 (ST51).

[0098] Thereby, CPU31 of IC card 4 records the client machine creation information supplied on RAM33 (ST52). Moreover, in parallel to supply of the information, by performing EXCLUSIVE OR operation for the user password with which the above-mentioned coincidence is judged, and the key information corresponding to a user currently recorded on EEPROM34 in advance with the master key generation vessel 36, CPU31 generates master key information as the result of an operation, and records it on RAM33 (ST53).

[0099] In the phase in which the above preparation was completed, CPU31 of IC card 4 transmits the Request to Send of the copy authorization code 43 to CPU10 of a client machine 1 (ST54). According to this Request to Send, CPU10 of a client machine 1 transmits the copy authorization code 43 to CPU31 of drawing and IC card 4 out of the control information 42 currently embedded in the encryption key information 41 (ST55).

[0100] Thereby, the copy authorization code 43 is in "1" and "0", and CPU31 of IC card 4 judges copy authorization or copy disapproval (ST56). When copy

authorization is judged as a result of this decision, CPU31 is unconditionally received, though the source of encryption information 40 grade is reproduced by the disk of HDD16 or an optical disk unit 17, and progresses to a decryption of latter step 61.

[0101] Since it is necessary to check the source of encryption information 40 grade when copy disapproval is judged as a result of decision of the above-mentioned step 56, CPU31 transmits the Request to Send of the drive code 44, an address code 45, and a region code 46 to CPU10 of a client machine 1 (ST57). According to this Request to Send, CPU10 of a client machine 1 transmits the drive code 44, an address code 45, and a region code 46 to CPU31 of drawing and IC card 4 out of the control information 42 currently embedded in the encryption key information 41 (ST58).

[0102] Thereby, CPU31 of IC card 4 checks coincidence with the drive code 44 supplied from a client machine 1, an address code 45, a region code 46, and the client machine creation information currently recorded on RAM33 (ST59).

[0103] That is, if sources, such as encryption information, are ISDN which is 10MHz, the drive code within client machine creation information will serve as "1 H", and sources, such as encryption information, will be judged to be right things in accordance with "1 H" of the drive code 44 of control information 42.

[0104] Moreover, when sources, such as encryption information, are reproduced from HDD16, since the drive code within client machine creation information serves as "CH" and is not in agreement with "1 H" of the drive code 44 of control information 42, sources, such as encryption information, are not right, that is, it is judged to be the information copied illegally.

[0105] Moreover, it is judged by whether the IP address of the transmitting origin within client machine creation information and the address code 45 of control information 42 are in agreement whether encryption information etc. is an original thing or the thing unjustly copied to commerce as a pirate edition.

[0106] By the above-mentioned step 59, when an inequality is judged, it considers that CPU31 is injustice, it suspends actuation, and notifies NG signal



to a client machine 1 (ST60). When coincidence is judged (when encryption information etc. is judged to be an original thing), or when copy authorization is judged by the above-mentioned step 56 by the above-mentioned step 59, CPU31 judges authorization of a decryption, judges initiation for a decryption, and transmits the Request to Send of the encryption key information 41 to CPU10 of a client machine 1 by it (ST61). According to this Request to Send, CPU10 of a client machine 1 transmits the encryption key information 41 to IC card 4 (ST62).

[0107] Thereby, CPU31 of IC card 4 makes the processing which decrypts encryption key information 41 supplied from a client machine 1 by the decoder 37 using the master key information currently recorded on RAM33 (decode) perform, generates key information, and records it on RAM33 (ST63).

[0108] Subsequently, CPU31 transmits the Request to Send of the encryption information 40 to CPU10 of a client machine 1 (ST64). According to this Request to Send, CPU10 of a client machine 1 transmits the encryption information 40 to IC card 4 (ST65).

[0109] Thereby, CPU31 of IC card 4 makes the processing which decrypts encryption information 42 supplied from a client machine 1 by the decoder 38 using the key information currently recorded on RAM33 (decode) perform, generates raw information, and transmits it to a client machine 1 (ST66).

[0110] According to transmission of this raw information, CPU10 of a client machine 1 records programs, such as word-processing software as transmitted raw information, on RAM22 (ST67). Consequently, it can process using programs, such as word-processing software currently recorded on RAM22 in the client machine 1.

[0111] As mentioned above, it is generable in the location which is not visible to a user with a master key generation vessel within IC card 4 in the master key information which is a common key using a user password.

[0112] Moreover, the key information corresponding to a user is beforehand recorded on EEPROM, a master key generation machine generates the master key information which is a common key from the user password entered by this

key information and user corresponding to a user, and the information enciphered by the decoder using this generated master key information is decrypted.

[0113] Since the encryption processing for every user demand of a host server becomes unnecessary as described above, information delivery is attained by low cost. Moreover, an informational illegal copy can be discovered very easily and security can be raised substantially.

[0114] If encryption is seen technically, compared with the conventional hybrid system of enciphering the data itself with a common key and enciphering only this common key again with a public key, a common key will be published to a duplex, signal transduction (transfer of the enciphered common key) of one common key will be carried out together with the data enciphered by enciphering, and the common key of another side will be decrypted within IC card 4 using the specific information from a user. For this reason, a common key is visible to a user's neither own in the middle of a transfer path.

[0115] Therefore, there are few dangers of being copied illegally according, to the 3rd person under transfer of 1. key to the fault of a common key system.

2. Management of a key is easy (a user should just have one IC card).

3. The alteration of the code data in a reception place is difficult. There is nothing only by being improved substantially, and compared with an ASHIN metric method, encryption/decryption processing is relatively easy for 4. information service provider side / user side, and it can be processed in a short time.

5. That an information service provider side should set up only a master key, since it is not necessary to ask the public key to the management center for every user, the information offer activity to a user can increase the efficiency substantially.

6. The information service provider side records the information enciphered in advance on the IC card side, and can deliver it as it is. For this reason, compared with the conventional cipher system which enciphers and carries out information delivery for every demand of a user, the burden by the side of an information

service provider improves substantially.

7. Preparation of a decryption is completed only in the conventional authentication procedure of entering a user password into the personal authentication using an IC card. Therefore, encoding technology can be adopted, without newly forcing a burden upon a user for security reservation.

8. Since the drive code and the address code are contained in the control information of encryption key information, the information enciphered by the user side is copied to HDD or an optical disk as it is, and it can prevent using improperly.

[0116] Consequently, all the faults of the conventional encoding technology are improved, and information sending origin and a reception place can simplify processing substantially, and can strengthen a security function. Next, the information (refer to drawing 2 ) which consists of encryption key information 41 that the encryption information 40 which was recorded on optical disk 17a, such as DVD-ROM, at the Records Department (HDD29) of the host server 3 of the 1st operation gestalt, and control information 42 are inserted in as the 2nd embodiment is recorded, and the case where load the optical disk unit (ROM drive) 17 of the client machine 1 of the 1st operation gestalt with this DVD-ROM17a, and it reproduces is explained.

[0117] In this case, "FH" which shows DVD-ROM as a drive code within control information is described, and the date of manufacture showing the stage when the original recording of an optical disk was created as a hour entry is described.

[0118] That is, the encryption information 40 and the encryption key information 41 that control information 42 is inserted in are reproduced from DVD-ROM17a with which the optical disk unit 17 was loaded instead of the communication link packet which consists of the encryption information 40, encryption key information 41 that control information 42 is inserted in, and an IP address being transmitted from a host server like the 1st operation gestalt. Subsequent actuation is processed almost like the case of the flow chart shown in drawing 13 and drawing 14 . However, when the drive code within client machine creation

information is set to "FH" and it is in agreement with "FH" of the drive code 44 of control information 42, sources, such as encryption information, are judged to be right things.

[0119] Moreover, as encryption information recorded on optical disk (DVD-ROM) 17a, video datas etc. may be other information besides a program etc. Moreover, it may not be made not to process the part related to a user password among the actuation shown in drawing 13 and drawing 14 (step 53). In this case, master key information is beforehand recorded on EEPROM34 by IC card 4 instead of the key information corresponding to a user.

[0120] Moreover, optical disk (DVD-ROM) 17a is created by being used at the time of the manufacture of optical disk (DVD-ROM) 17a shown below, and recording those information as well as record to HDD29 of the encryption key information 41 that the encryption information 40 which used and explained drawing 10 of the 1st example - drawing 12 , and control information 42 are inserted in on original recording 70.

[0121] The manufacture approach of the above-mentioned optical disk (DVD-ROM) 17a is explained using (k) from (a) - (e) of drawing 15 , and (f) of drawing 16 . In order to guarantee surface precision, the glass plate 71 made with tempered glass with a thickness of 0.5-30mm is put on a spindle motor 72 ((a) of drawing 15 ), and is rotated at a specific rotational frequency. From moreover, the photoresist liquid melted by the organic solvent is sprinkled and photoresist liquid is opened to homogeneity using the centrifugal force by revolution of a glass plate 71. As generally as a spinner coating method, this applying method is called. Elevated-temperature neglect is carried out after that at every glass plate 71 60-300-degreeC, an organic solvent is evaporated, and the photoresist layer 73 of the uniform thickness dr is formed ((b) of drawing 15 ).

[0122] (f) of drawing 16 mentioned later - drawing 16 Although imprint effectiveness falls at the process of (i), when the imprint effectiveness in a stroke is 100% temporarily, the thickness dr of this photoresist layer 73 becomes the pit depth or the PURIGURUBU depth on the record film 84 of a final information

record medium.

[0123] Then, with the original recording apparatus mentioned later, a laser beam 75 is made to condense with an objective lens 76, a photoresist layer 73 is exposed intermittently, and the exposure section 74 is created ((c) of drawing 15 ). If the exposure over the perimeter is completed, it will remove from an original recording device the whole glass plate 71, and a developer 77 is sprinkled specific time, rotating a glass plate 71, as shown in (d) of drawing 15 .

[0124] Then, as shown in (e) of drawing 15 , the exposure section 74 carries out \*\*\*\*\* lack, and the minute irregularity of a level difference  $\Delta r$  is done. Thus, the glass plate 71 and photoresist layer 73 which were done are called the original recording 70 of an optical disk. Thus, the created original recording 70 is removed from a spindle motor 72, and the replica of the concavo-convex configuration of original recording 70 is taken by the electroless deposition by nickel, and electrolytic plating (electrocasting plating). Drawing 16 The replica which carried out in this way and was formed as shown in \*\* (f) is called the master plate 78. If master plate 78 creation is completed, it will attach into organic solvents, such as an acetone, a photoresist layer 73 will be melted, and the master plate 78 will be exfoliated from original recording 70. After creating the mother plate 79 by electrolytic plating (electrocasting plating) after that based on the master plate 78 ((g) of drawing 16 ), the mother plate 79 is exfoliated from the master plate 78. It carries out again based on the mother plate 79, and La Stampa 80 is created by electrolytic plating (electrocasting plating) ((h) of drawing 16 ).

[0125] Generally the transparence plastic plate 83 of an information record medium is created using the approach called "injection molding." that is, metal mold A81 and metal mold B82 are arranged for the business of (i) of drawing 16 , and the resin material (generally a polycarbonate, PMMA, and ABS are used as the material of construction in many cases) which looked like [ the clearance between in the meantime ] muddily, and was melted at the elevated temperature

in it is pushed in. Since attach and La Stampa 80 created at the above-mentioned process is in metal mold A81, the minute concavo-convex configuration of La Stampa 80 is imprinted by resin material in the phase where resin material was pushed in. Then, it is left several minutes and resin material is cooled to ordinary temperature metal mold A81 and the whole metal mold B82, when resin material got cold and solidified, between metal mold A81 and metal mold B82 is extended, and a plastic plate 83 (the resin material by which the above got cold and the lump and the concavo-convex configuration were imprinted is called the plastic plate 83) is taken out.

[0126] Thus, the obtained plastic plate 83 is arranged in a vacuum, record film 84 is formed on a plastic plate 83 by vacuum evaporation of spatter vacuum evaporation, vacuum deposition, ion plating, etc., and structure like (j) of drawing 16 is made. Thus, the created object is arranged so that two-sheet record film 84 and 86 may become inside, the meantime is filled up with record film 84, and an information record medium like (k) of drawing 16 is completed.

[0127] The structure of an original recording recording device of making the photoresist layer 73 shown by (c) of drawing 15 exposing locally is shown in drawing 17. As mentioned above, a glass plate 71 rotates at a specific rotational frequency on a spindle motor 72. A laser beam 75 condenses on a photoresist layer 73 with the objective lens 76 after an echo by the clinch mirror 88. The clinch mirror 88 and an objective lens 76 are united as moving part 89, and move to radial [ of a glass plate 71 ]. This moving part 89 moves by the delivery motor 90 and the delivery gear 91. Although not illustrated, it had the monitor part which carries out the monitor of the condensing spot location on a glass plate 76 optically, the rotational frequency of a spindle motor 72 changed according to this monitor output, and the original recording record control section 50 has controlled so that the passing speed (linear velocity) of the relative condensing spot on a glass plate 71 always becomes fixed.

[0128] The laser beam 75 which came out of the laser light source 97 reaches the E.O. modulator 94 and the A.O. modulator 93 to the clinch mirror 88 after

passage. The PURIPITTO signal which is a minute concavo-convex pit configuration embraces the signal of PURIPITSU \*\*\*\*\* 99, switches on / turns off the high-speed switch 96, and the electrical potential difference of the adjustable voltage generator 95 is impressed to the E.O. modulator 94, or it releases it. If the applied voltage to this E.O. modulator 94 is changed, the laser intensity which passes the E.O. modulator 94 will change. Thus, the laser intensity which reaches to a photoresist layer 73 is changed, and the exposure section 74 on a photoresist layer 73 and a non-exposed area are made.

[0129] A standing wave (A. compressional wave between the molecules in 93 O. modulators) with the specific distance-period in the A.O. modulator 93 occurs by applying the electrical potential difference of a specific frequency to the A.O. modulator 93 with the specific frequency oscillator 92. A laser beam 75 receives a black (Bragg) echo by this standing wave, and it is bent in the specific direction. Therefore, when the distance-period of this standing wave changes, black (Bragg) conditions change and the include angle a laser beam 75 turns also changes. That is, by changing the output frequency of the specific frequency oscillator 92, the travelling direction of a laser beam 75 changes and, as a result, a condensing point location moves radially on a photoresist layer 73.

[0130] according to the output of a WOBURU groove generator / groove pit switcher 98, with a specific period, in the case of the information record medium which has the structure in which PURIGURUBU carries out specific period meandering, the frequency of the frequency oscillator 92 changes, and it comes out and requires it. Moreover, in the case of a WO bull pit, only as for the one half of a track pitch (pitch between land grooves), a condensing spot changes the frequency of the specific frequency oscillator 92 so that it may shift radially on a photoresist layer 73.

[0131] or [ that information playback is independently possible for the ROM drive 17 (client machine 1) with no decryption means for decrypting encryption information as described above ] -- it can judge whether it is prohibition. When prohibition of information playback is detected, it can avoid transmitting by this

the information to which playback and a transfer were forbidden to equipments, such as a personal computer which performs decryption processing and regeneration after it.

[0132] Moreover, although the conventional thing has the fault cost also increases in \*\*\*\* and it becomes impossible to also take compatibility with the conventional ROM drive and to say if it does not give a decryption means to decrypt key information in a ROM drive when control information is included in the key after a decryption, it can avoid such a fault in the 2nd embodiment of the above.

[0133] Moreover, as other embodiments, as shown in drawing 18 , the case of the network system by which the host server 101 and the server 102 for users are connected with the network computer 105 through networks 103 and 104, respectively is explained.

[0134] For example, a host server 101 is the same configuration as the host server 3 of the 1st operation gestalt, and has HDD 29 on which the information which consists of encryption key information 41 that the key information which control information 42 is inserted in in the form un-enciphered as the programs (information which a user uses) 40, such as word-processing software enciphered as encryption information, and decrypts the encryption information 40 (decode) is enciphered is recorded.

[0135] A network computer 105 By the decryption section 108 and the decryption section 108 which decode codes, such as encryption information received in the receive section 107 which receives the encryption information from a control section 106 and the host server 101 which controls the whole network computer 105, and the receiving receive section 107 The dispatch section 111 which disseminates information to the server 102 for users constitutes the processing result enciphered with RAM memory 109 which records the decoded information, the code machine 110 which enciphers the processing result by the control section 106, and the code vessel 110. It has the 1st same configuration and same function as IC card 4 of an operation gestalt, and, as for the above-



mentioned decryption section 108, the code machine 110 also has the 1st same configuration and same function as the code machine 24 of an operation gestalt.

[0136] The encryption information on the small-scale functional program described by this by JAVA sent via a network 102 from the host server 101 etc. is changed into an electrical signal in a receive section 107, it is inputted into the decryption section 108 as it is, and the functional program after a decryption is inputted into RAM memory 109. Data processing is carried out in a control section 106, reading a functional program from RAM memory 109. The result after processing is sent to the server 102 for users via a network 103 from the dispatch section 111, after being enciphered with the code vessel 110.

[0137] Since all the circuits except the receive section 107 and the dispatch section 111 in a network computer 105 are one-chip-ized, the raw signal after a decryption has structure which cannot be taken out out of direct, and security is strengthened further.

[0138] Moreover, the example using a broadcasting satellite is explained as other embodiments using drawing 19 . That is, encryption information as shown in drawing 2 of the 1st operation gestalt via a broadcasting satellite 122 from a key station 121 etc. is sent. It is decrypted by the raw signal in the decryption section 125 formed with the IC card of the 1st operation gestalt after changing into an electrical signal in the receive section 124 in the information regenerative apparatus 123, and is displayed by the display 126. According to each embodiment mentioned above, security reservation is required or can prevent the unjust duplicate about the information which needs copyright reservation.

[0139]

[Effect of the Invention] Since the encryption processing for every user demand of a host server becomes unnecessary according to this invention as explained in full detail above, information delivery is attained by low cost. According to this invention, an informational illegal copy can be discovered very easily and security can be raised substantially.

[0140] According to this invention, to the fault of a common key system, there are

few dangers by the 3rd person under transfer of a key of being copied illegally, management of a key is easy, and the point said that the alteration of the code data in a reception place is difficult is improved substantially.

[0141] According to this invention, compared with an ASHIN metric method, the point shown below is improved substantially. Encryption/decryption processing is relatively easy for provider side / user side of data utility, and it can be processed in a short time.

[0142] That an information service provider side should set up only a master key, since it is not necessary to ask the public key to the management center for every user, the information offer activity to a user can increase the efficiency substantially.

[0143] The information service provider side records the information enciphered in advance on the IC card side, and can deliver it as it is. For this reason, compared with the conventional cipher system which enciphers and carries out information delivery for every demand of a user, the burden by the side of an information service provider improves substantially.

[0144] Preparation of a decryption is completed only in the conventional authentication procedure of entering a user password into the personal authentication using an IC card. Therefore, encoding technology can be adopted, without newly forcing a burden upon a user for security reservation.

[0145] Since device information and field information are included in the control information of encryption key information, the information enciphered by the user side is copied to HDD or an optical disk as it is, and it can prevent using improperly. Consequently, all the faults of the conventional encoding technology are improved, and information sending origin and a reception place can simplify processing substantially, and can strengthen a security function.

---

[Brief Description of the Drawings]

[Drawing 1] Drawing 1 is drawing showing the outline configuration of the information transmission system for explaining the gestalt of implementation of this invention.

[Drawing 2] Drawing 2 is drawing showing the example of structure of service information.

[Drawing 3] Drawing 3 is drawing showing the example of a configuration of control information.

[Drawing 4] Drawing 4 is the perspective view showing the configuration of the IC card of drawing 1 .

[Drawing 5] Drawing 5 is the block diagram showing the outline configuration of the client machine of drawing 1 .

[Drawing 6] Drawing 6 is the block diagram showing the outline configuration of the host server of drawing 1 .

[Drawing 7] Drawing 7 is the block diagram showing the outline configuration of the key information-synthesis machine of drawing 6 .

[Drawing 8] Drawing 8 is the block diagram showing the outline configuration of the code machine of drawing 6 , and a decoder.

[Drawing 9] Drawing 9 is the block diagram showing the outline configuration of the IC card of drawing 1 .

[Drawing 10] Drawing 10 is a flow chart for explaining the record approach of service information.

[Drawing 11] Drawing 11 is drawing showing the generation process of encryption key information and encryption information.

[Drawing 12] Drawing 12 is a flow chart for explaining the registration approach into the IC card of the key information corresponding to a user.

[Drawing 13] Drawing 13 is a flow chart for explaining the processing which decodes the information which is acquired according to a demand, and which is enciphered with an IC card, and is set up as a functional program.

[Drawing 14] Drawing 14 is a flow chart for explaining decryption processing of encryption information.

[Drawing 15] Drawing 15 is drawing for explaining the manufacture approach of DVD-ROM.

[Drawing 16] Drawing 16 is drawing for explaining the manufacture approach of DVD-ROM.

[Drawing 17] Drawing 17 is drawing for explaining the outline configuration of an original recording recording device.

[Drawing 18] Drawing 18 is drawing showing the outline configuration of the network system for explaining other embodiments.

[Drawing 19] Drawing 19 is drawing showing the example using the broadcasting satellite for explaining other embodiments.

[Description of Notations]

1 -- Client machine

2 -- Communication line

3 -- Host server

4 -- IC card

29 -- Records Department (HDD)

40 -- Encryption information

41 -- Encryption key information

42 -- Control information

---